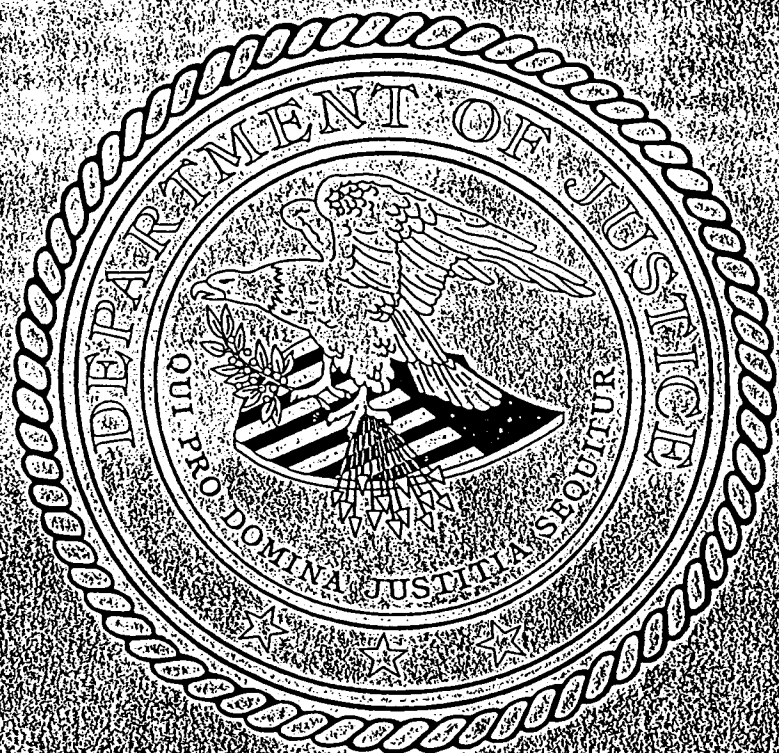


Electronics Surveillance Manual Procedures and Case Law Forms



Prepared By
Electronic Surveillance Unit
Office of Enforcement Operations

Revised October 1997
(Complete in one volume)

FOREWORD

This manual was prepared by the Electronic Surveillance Unit, Office of Enforcement Operations, Criminal Division, and is designed primarily to assist federal prosecutors and investigative agents in the preparation of electronic surveillance applications made pursuant to Title 18, United States Code, Sections 2510-2522 (1996) ("Title III") and associated statutes. It is not intended to confer any rights, privileges, or benefits upon defendants, nor does it have the force of a United States Department of Justice directive. See United States v. Caceres, 440 U.S. 741 (1979). In addition to outlining and discussing the statutory requirements of Title III applications, this manual also sets forth the Department's authorization process, provides guidance in filing Title III pleadings before the court, and discusses the applicable case law as well as both novel, and frequently arising, legal issues involved in Title III litigation. Samples of the most commonly filed pleadings follow the text.

INTRODUCTION

This manual sets forth the procedures established by the Criminal Division of the Department of Justice to obtain authorization to conduct electronic surveillance pursuant to Title 18, United States Code, Sections 2510-2522 (1996) (Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986 (ECPA), the Communications Assistance for Law Enforcement Act of 1994 (CALEA), and the Antiterrorism and Effective Death Penalty Act of 1996 (Antiterrorism Act)), and discusses the statutory requirements of each of the pleadings. Throughout this manual, the above federal wiretap statutes will occasionally be referred to collectively as "Title III."

This manual is divided into two sections. The first section provides an overview of the procedures to follow when applying for authorization to conduct electronic surveillance, and discusses format, statutory and policy requirements, and pertinent case law concerning specific electronic surveillance issues. The second section provides sample forms pertaining to electronic surveillance involving wire, oral and electronic communication interceptions, pen register/trap and trace procedures, access to transactional data and stored electronic communications, and the use of tracking devices. These forms are intended only to provide general guidance in drafting the most frequently used pleadings and do not prohibit alternative approaches.

TABLE OF FORMS

Application for Wire/Oral Interception	45
Affidavit for Wire/Oral Interception	51
Order for Interception of Wire/Oral Communications	60
Order to Service Provider	65
Minimization Instructions	67
Application for Electronic Communications Interception	72
Affidavit for Electronic Communications Interception	76
Order for Electronic Communications Interception	85
Application for Sealing	88
Order for Sealing	90
Application for § 2703(d) Court Order	92
Section 2703(d) Court Order	94
Application for Trap and Trace/Pen Register	96
Order for Trap and Trace/Pen Register	99
Application for Video Surveillance	102
Order for Video Surveillance	105
Application for Disclosure	107
Order for Disclosure	110
Section 2517(5) Application for Testimonial Use of Interceptions Relating to "Other Offenses"	112
Section 2517(5) Order Permitting Testimonial Use of Interceptions Relating to "Other Offenses"	114
Inventory Application	116
Order for Inventory	117
Inventory Notice	118
Application for Destruction of Tapes	119

Order for Destruction of Tapes	121
Affidavit for Mobile Tracking Device	123
Order for Mobile Tracking Device	125

I. THE ELECTRONIC SURVEILLANCE UNIT

The Electronic Surveillance Unit (ESU) operates within the Office of Enforcement Operations (OEO), Criminal Division, and handles all requests made pursuant to Title III to conduct non-consensual, domestic surveillance of wire, oral, and electronic communications for law enforcement purposes. The ESU does not handle state wiretaps or requests to conduct domestic national security electronic surveillance pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. §§ 1801, et seq.) (FISA). Questions concerning FISA taps should be directed to the Office of Intelligence and Policy Review at (202) 514-5600.

Attorneys in the ESU are responsible for reviewing and processing all Title III requests, and are available to assist in the preparation of Title III applications and to answer questions on any Title III-related issue. All such inquiries should be directed to (202) 514-6809. ESU attorneys will also provide assistance in responding to suppression motions and preparing briefs on Title III issues. For assistance in this area, contact the Chief or Deputy Chief of the ESU at the above number.

II. TITLE III AUTHORIZATION PROCESS

The following is a brief explanation of the Department of Justice's procedures for reviewing and authorizing Title III applications.

1. A copy of the proposed order, application, and affidavit is submitted to the ESU and to the Washington, D.C., office of the investigative agency handling the case. Those pleadings should be sent to the Office of Enforcement Operations, Electronic Surveillance Unit, 1001 G Street, N.W., Suite 900 West, Washington, D.C. 20001, and should be sent via overnight mail. If the documents are short enough, they may be faxed directly to the ESU at (202) 616-2010. For security reasons, these pleadings may not be sent via e-mail.

Except in the case of genuine emergencies, discussed below, most original applications require approximately one week to review and process from the time the ESU receives the affidavit. Spinoff requests (i.e., applications to conduct electronic surveillance at a new location or over a new facility that are related to an ongoing or previously conducted interception reviewed by the ESU) are considered original applications and are reviewed and processed in the same manner described below, and require agency approval. Extension requests (i.e., applications to continue interceptions over the same facility or premises) require review only by the ESU, and not the investigative agency. Because the ESU is presently reviewing approximately 1,400 Title III applications per year, it is imperative when coordinating an

investigation or planning extension requests that sufficient time is allowed for the Title III application to be reviewed by both the ESU and, when appropriate, the investigative agency.

2. When an application is received in the ESU, it is logged in and assigned to one of the reviewing attorneys. This attorney will be responsible for reviewing all spinoffs and extensions arising from the original application. The attorney will discuss with the Assistant United States Attorney (AUSA) handling the case any necessary changes or additions to the affidavit, and will coordinate the processing of the request with the investigative agency's Office of Legal Counsel or, in the case of the FBI, the appropriate section within the Criminal Investigative Division. Once the affidavit has been reviewed by both the ESU attorney and the investigative agency's counsel and is in final form, the head of the investigative agency will send, through the ESU, a memorandum to the Assistant Attorney General (or Acting Assistant Attorney General) for the Criminal Division requesting that electronic surveillance be authorized in this case. Because it is the investigative agency that has the ultimate responsibility for conducting the requested electronic surveillance, the ESU cannot recommend approval of a Title III until this agency memorandum has been finalized. (The agency memorandum is required only for original applications and spinoff applications involving a new facility or location; it is not required for an extension request.) Minor changes or additions to the affidavit can usually be faxed to the ESU and the investigative agency for insertion in the original; however, in those cases when an affidavit needs substantial revision, a new copy must be submitted. Generally, an AUSA's only contact person will be the ESU attorney assigned to the case. Any problems or changes requested by the investigative agency's counsel will be communicated to the affiant by the agency after consultation with the ESU attorney.

3. After reviewing the application, the ESU attorney will write an action memorandum to the Assistant Attorney General (AAG), Criminal Division, summarizing and analyzing the relevant facts and legal issues as they pertain to the proposed electronic surveillance, and discussing the application's compliance with the statutory requirements of Title III. This memorandum also contains the ESU's recommendation of approval or disapproval of the application. Once the reviewing attorney has written the action memorandum, a package is prepared containing the memorandum and the pleadings. This package, together with the requesting memorandum from the head of the investigative agency, is then sent to the AAG's office for final review and authorization.

4. If the application is approved, the ESU will fax the AUSA the following items: the authorization document, which is a memorandum from a properly designated official to the Director of

OEO, authorizing Title III surveillance; a copy of the Attorney General's most recent delegation order, which identifies those individuals to whom the Attorney General has delegated authority to authorize Title III applications; and a letter from the AAG (signed by the Director of OEO) to the United States Attorney, confirming that the requested Title III authorization has been granted. Both the AAG's authorization memorandum and the copy of the delegation order should be filed with the pleadings; the letter to the United States Attorney is solely for the AUSA's files.

III. THE ELECTRONIC SURVEILLANCE PLEADINGS

Discussed below are the requirements for each of the three documents comprising a Title III application: the Application, the Affidavit, and the Order. These requirements, which are set forth in 18 U.S.C. § 2518, are applicable to requests for oral, wire and electronic communications. Samples of each of these pleadings are found in the Forms section.

1. The Application

a. It must identify the applicant (an AUSA) as a law enforcement or investigative officer, and must be in writing, signed by the AUSA and made under oath. 18 U.S.C. § 2518(1). It must be presented to a federal district court or court of appeals judge, and be accompanied by the Department's authorization memorandum signed by an appropriate Department of Justice official. See 18 U.S.C. §§ 2516(1) and 2510(9)(a); In re United States, 10 F.3d 931 (2d Cir. 1993) (explaining that "judge of competent jurisdiction" does not include magistrate judges), cert. denied sub nom. Korman v. United States, 513 U.S. 812 (1994).

b. It must identify the type of communications to be intercepted. 18 U.S.C. § 2518(1)(b)(iii). "Wire communications" are "aural transfers" (involving the human voice) that are transmitted, at least in part by wire, between the point of origin and the point of reception, i.e., telephone calls. 18 U.S.C. § 2510(1). This includes voice communications conducted over cellular telephones, cordless telephones and voice pagers, as well as over traditional landline telephones. "Oral communications" are only treated as such by Title III when they involve utterances by a person exhibiting a reasonable expectation of privacy, such as conversations within a person's residence, private office, or car. 18 U.S.C. § 2510(2). An "electronic communication" most commonly involves digital display paging devices and electronic facsimile machines, but also includes electronic mail and computer transmissions. It does not include communications made through tone-only paging devices, communications from a tracking device, or electronic funds transfer information. 18 U.S.C. § 2510(12).

c. It must identify the specific federal offenses for which the affidavit sets forth probable cause to believe have been, are being, or will be committed. 18 U.S.C. § 2518(1)(b)(i). The offenses that may be the predicates for a wire or an oral interception order are limited to those set forth in 18 U.S.C. § 2516(1). In the case of electronic communications, a request for interception may be based on any federal felony, pursuant to 18 U.S.C. § 2516(3).

d. It must provide a particular description of the nature and location of the facilities over which, or the place where, the interception is to occur. 18 U.S.C. § 2518(1)(b)(ii). Specifically excepted from the particularity requirement of 18 U.S.C. § 2518(1)(b)(ii) are the roving interception provisions set forth in 18 U.S.C. § 2518(11). See also 18 U.S.C. § 2518(12). The specific requirements of the roving provisions are discussed in detail below. Briefly, in the case of a roving oral interception, the application must show, and the order must state, that it is impractical to specify the locations where the oral communications of a particular named subject or subjects are to be intercepted. 18 U.S.C. 2518(11)(a)(ii), (iii). In the case of a roving wire or electronic interception, the application must show, and the order must find, that a particular named subject (or subjects) is (are) using various and changing facilities for the purpose of thwarting electronic surveillance. 18 U.S.C. § 2518(11)(b)(ii), (iii). In the case of a roving interception, the accompanying DOJ authorization document must be signed by an official at the Assistant Attorney General or acting Assistant Attorney General level or higher. 18 U.S.C. § 2518(11)(a)(i), (b)(i).

e. It must identify the person(s), if known, committing the offenses and whose communications are to be intercepted. 18 U.S.C. § 2518(1)(b)(iv); United States v. Donovan, 429 U.S. 413 (1977). It is the Department's policy to name in the pleadings all persons as to whom there is probable cause to believe are committing the offenses ("violators"), and then to delineate who among the violators will be intercepted over the target facilities discussing the offenses ("interceptees"). (Typically, the list of interceptees is nothing more than a subset of the larger list of violators.) It is also Department policy to name individuals in Title III pleadings even if their involvement does not rise to the level of probable cause. See United States v. Ambrosio, 898 F. Supp. 177 (S.D.N.Y. 1995) ("since nothing in the statute restricts the government from naming in the affidavit individuals as to whom it may not have probable cause, the statute's goal of providing [inventory] notice [of the wiretap pursuant to 18 U.S.C. § 2518(8)(d)] is actually furthered by naming more, rather than fewer, persons"). See also United States v. Martin, 599 F.2d 880 (9th Cir.), cert. denied, 441 U.S. 962 (1979) (same).

f. It must contain a statement affirming that normal investigative procedures have been tried and failed, or are reasonably unlikely to succeed, or are too dangerous to employ. 18 U.S.C. § 2518(1)(c). The applicant may then state that a complete discussion of attempted alternative investigative techniques is set forth in the accompanying affidavit.

g. It must contain a statement affirming that the affidavit contains a complete statement of facts concerning all previous applications that have been made to intercept the oral, wire, or electronic communications of any of the named persons or involving the target facility or location. 18 U.S.C. § 2518(1)(e); United States v. Bianco, 998 F.2d 1112 (2d Cir. 1993) (holding that the duty to disclose prior applications covers all persons named in the application and not just those designated as "principal targets"), cert. denied, 511 U.S. 1069 (1994); United States v. Ferrara, 771 F. Supp. 1266 (D. Mass. 1991) (when "the government has decided to name in its Application individuals believed to be co-conspirators of the proposed principal targets of an interception order, it has an obligation to inform the issuing judge of all prior requests for authority to intercept communications of those individuals").

h. If involving an oral (and occasionally a wire or an electronic) interception, it must contain a request that the court issue an order authorizing investigative agents to make surreptitious and/or forcible entry to install, maintain, and remove electronic interception devices in or from the targeted premises. In effecting this, the applicant should notify the court as soon as possible after each surreptitious entry.

i. If involving a wire interception (and an electronic interception involving, for example, a facsimile machine), it must contain a request that the authorization apply not only to the target telephone number, but to any changed telephone number subsequently assigned to the same cable, pair, and binding posts used by the target landline telephone within the thirty (30) day interception period. With regard to cellular telephones, the language should read: "... but to any changed telephone number or any other telephone number assigned to or used by the instrument bearing the same electronic serial number used by the target cellular telephone within the thirty (30) day period." The application should also request that the authorization apply to background conversations intercepted in the vicinity of the target telephone while the telephone is off the hook or otherwise in use. See United States v. Baranek, 903 F.2d 1068, 1071-72 (6th Cir. 1990) (aural version of the "plain view" doctrine applied).

j. If involving a wire (and sometimes an electronic) interception, it must also contain a request that the court issue an order directing the service provider, as defined in 18 U.S.C.

§ 2510(15), to furnish the investigative agency with all information, facilities, and technical assistance necessary to facilitate the ordered interception. 18 U.S.C. §§ 2511(2)(a)(ii) and 2518(4). The application should also request that the court order the service provider and its agents and employees not to disclose the contents of the court order or the existence of the investigation. 18 U.S.C. § 2511(2)(a)(ii).

k. It should contain a request that the court's order be issued for a period not to exceed thirty (30) days, measured from the earlier of the day on which the interception begins or ten (10) days after the order is entered, and that the interception must terminate upon the attainment of the authorized objectives. 18 U.S.C. § 2518(1)(d), (5).

l. It should contain a statement affirming that all interceptions will be minimized in accordance with Chapter 119 of Title 18, United States Code, as described further in the affidavit.

2. The Affidavit

a. It must be sworn and attested to by an investigative or law enforcement officer, as defined in 18 U.S.C. § 2510(7). Department policy precludes the use of multiple affiants except when it is indicated clearly which affiant swears to which part of the affidavit, or that each affiant swears to the entire affidavit. If a state or local law enforcement officer is the affiant for a federal electronic surveillance affidavit, he must be deputized as a federal officer of the agency with responsibility for the offenses under investigation. See 18 U.S.C. § 2516(1) (interceptions are to be conducted by the federal agency responsible for the offenses for which the application is made); United States v. Lyons, 695 F.2d 802 (4th Cir. 1982) (judge was aware that state and local law enforcement officials were part of a DEA task force and that they would be monitoring the wire under the supervision of the DEA, the federal agency ordered to conduct the interception). Section 2518(5) permits non-officer "Government personnel" or individuals acting under contract with the government to monitor conversations pursuant to the interception order. These individuals must be acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception when monitoring communications, and the affidavit should note the fact that these individuals will be used as monitors pursuant to section 2518(5). Department of Defense personnel would appear to qualify as "Government personnel" and could, therefore, without deputization, assist in the Title III monitoring process (e.g., as translators), if such assistance does not violate the Posse Comitatus laws ("PCA"), 10 U.S.C. § 375 and 18 U.S.C. § 1385, and related regulations, 32 C.F.R. § 213.10(a)(3), (7). An opinion issued by the Office of Legal Counsel ("OLC"), Department of

Justice, dated April 5, 1994, concluded that such assistance by military personnel would not violate the PCA. The OLC analysis did not extend to National Guard personnel, who are considered state employees rather than Federal Government personnel. Consequently, use of members of the National Guard will require that they be deputized as law enforcement officers or placed under contract. A copy of the OLC opinion may be obtained from the ESU. See generally United States v. Al-Talib, 55 F.3d 923 (4th Cir. 1995); United States v. Khan, 35 F.3d 426 (9th Cir. 1994); United States v. Yunis, 924 F.2d 1086 (D.C. Cir. 1991); Hayes v. Hawes, 921 F.2d 100 (7th Cir. 1990).

b. It must identify the subjects, describe the facility or location that is the subject of the proposed electronic surveillance, and list the alleged offenses.

c. It must establish probable cause that the named subjects are using the targeted telephone(s) or location(s) to facilitate the commission of the stated offenses.

Any background information needed to understand the instant investigation should be set forth briefly at the beginning of this section. The focus, however, should be on recent and current criminal activity by the subjects, with an emphasis on their use of the target facility or location to facilitate this activity. This is generally accomplished through information from an informant, cooperating witness, or undercover agent, combined with pen register information or other telephone records for the target telephone, or physical surveillance of the target premises. It is Department policy that pen register or telephone toll information for the target telephone, or physical surveillance of the target premises, standing alone, is generally insufficient to establish probable cause.

Probable cause to establish criminal use of the facilities or premises requires independent evidence of use in addition to pen register or surveillance information, e.g. informant or undercover information. (It is preferable that all informants used in the affidavit to establish probable cause be qualified according to the "Aguilar-Spinelli" standards (Aguilar v. Texas, 378 U.S. 108 (1964) and Spinelli v. United States, 393 U.S. 410 (1969)), rather than those set forth in the more recent Supreme Court decision of Illinois v. Gates, 463 U.S. 1237 (1983).) On rare occasions, criminal use of the target facilities or premises may be established by an extremely high volume of calls to known or suspected coconspirators or use of the premises by them that coincides with incidents of illegal activity. It is Department policy that the affidavit reflect use of the target telephone or premises within twenty-one days of the date on which the Department authorizes the filing of the application. The subjects' use of the target facilities or premises within the twenty-one-day period may be evidenced through pen register

information and/or physical surveillance that updates earlier use. Historical information (i.e., information older than six months from the date of the application), combined with pen register information or physical surveillance alone, is generally insufficient to establish probable cause. Pen register information and physical surveillance not only serve to update the probable cause as to the criminal use of a telephone or premises, but also are required (in the absence of other information) to establish the need for the proposed electronic surveillance by demonstrating what types of criminal communications are expected to be intercepted over the telephone or within the premises during the thirty-day authorization period.

d. It must explain the need for the proposed electronic surveillance and provide a detailed discussion of the other investigative procedures that have been tried and failed, are reasonably unlikely to succeed, or are too dangerous to employ in accomplishing the goals of the investigation. It need not be shown that no other normal investigative avenues are available, only that they have been tried and proven inadequate or have been considered and rejected for the reasons described. There should also be a discussion as to why electronic surveillance is the technique most likely to succeed. When drafting this section of the affidavit, the discussion of other investigative techniques should be augmented with facts particular to the specific investigation and subjects. General declarations about the exhaustion of alternative techniques will not suffice. It is most important that this section be tailored to the facts of the specific case and be more than a recitation of boilerplate language. The affidavit must discuss the particular problems involved in the investigation in order to fulfill the requirement of section 2518(1)(c). It should explain specifically why investigative techniques, such as physical surveillance or the use of informants and undercover agents, are inadequate in the particular case. For example, if physical surveillance is impossible or unproductive because the suspects live in remote areas or will likely be alerted to law enforcement's presence, the affidavit should set forth those facts clearly. If the informants refuse to testify or cannot penetrate the hierarchy of the criminal organization involved, the affidavit should explain why that is the case in this particular investigation. If undercover agents cannot be used because the suspects deal only with trusted associates, the affidavit must so state and include the particulars. It is not enough, for example, to state that the use of undercover agents is always difficult in organized crime cases because organized crime families, in general, deal only with trusted associates. While the affidavit may contain a general statement regarding the impossibility of using undercover agents in organized crime cases, it must also demonstrate that the subject or subjects in the instant case deal only with known associates. The key is to tie the inadequacy of a specific

investigative technique to the particular facts underlying the investigation. See United States v. London, 66 F.3d 1227 (1st Cir. 1995) (the government must make "a reasonable good faith effort to run the gamut of normal investigative procedures before resorting to" electronic surveillance), cert. denied, 116 S. Ct. 1542 (1996); United States v. Mondragon, 52 F.3d 291 (10th Cir. 1995) (because the affidavit contained no alternative investigative need statement, the evidence was suppressed); United States v. Ashely, 876 F.2d 1069 (1st Cir. 1989) ("conclusory statements that normal investigative techniques would be unproductive, based solely on an affiant's prior experience, do not comply with the requirements of section 2518(1)(c)"); United States v. Santora, 600 F.2d 1317 (9th Cir. 1979) (evidence was suppressed because the government failed to show exhaustion of alternative investigative techniques for each new facility to be tapped); United States v. Castillo-Garcia, 920 F. Supp. 1537 (D. Colo. 1996) (successive affidavits failed to set forth specific facts demonstrating exhaustion of alternative techniques and continuing need; the affidavits were merely "boilerplate clones" of one another), modified, 117 F.3d 1179 (10th Cir. 1997).

e. It must contain a full and complete statement of any prior electronic surveillance involving the persons, facilities, or locations specified in the application. 18 U.S.C. § 2518(1)(e). This statement should include the date, jurisdiction, and disposition of previous applications, as well as their relevance, if any, to the instant investigation. In addition to any known prior applications, the agency conducting the investigation should run an "ELSUR" check of its own electronic surveillance indices, the indices of any other participating agency, and the indices of any agency which would likely have investigated the subjects in the past. In narcotics investigations, it is the Department's policy that the Drug Enforcement Administration, the Federal Bureau of Investigation, and the United States Customs Service conduct an ELSUR check to determine if any prior related electronic surveillance has been conducted.

f. It must contain a statement of the period of time for which the interception is to be maintained. 18 U.S.C. § 2518(1)(d). Section 2518(5) provides that an order may be granted for no longer than is necessary to achieve the objectives of the investigation, or in any event no longer than thirty (30) days, whichever occurs first. The statute further provides that the thirty-day period begins on either the day on which investigative officers first begin to conduct the interception or ten days after the order is entered, whichever is earlier. This ten-day grace period is intended primarily for the installation of oral monitoring equipment (microphones), allowing investigators time to break and enter, if necessary, and set up the equipment before the thirty-day period begins to be

calculated. This provision may also be used when delays arise in installing monitoring devices used in wire or electronic interceptions. In either case, the provision is not intended to provide an additional ten-day start-up period on a regular basis throughout the investigation; any delays that are encountered should be real and defensible if challenged. Accordingly, the ten-day grace period would normally apply only to the initial installation of equipment and should not be invoked in the following circumstances: 1) when an extension order has been obtained and the equipment has remained in place; 2) for an original application when the equipment has already been installed, or 3) in wire or electronic interception cases when a pen register or other device permitting almost immediate access to the target facility is already in place. The time will then run from the earlier of the day on which the interceptions begin (the time at which the monitoring equipment is installed and activated), or ten days after the order is entered. Because the language of section 2518(5) does not describe precisely the exact point (clock time or calendar day) from which the interception period is to be computed, the Department recommends that the thirty-day period be calculated as thirty, twenty-four hour periods from the earlier of the date and time the monitoring equipment is activated (if within the ten-day grace period), or ten days after the order is signed (if the ten-day grace period applies). With extension applications, because the monitoring equipment is already in place and can be easily activated, the thirty-day period should be calculated from the date and time the order is signed.

g. It must contain a statement affirming that monitoring agents will minimize all interceptions in accordance with Chapter 119 of Title 18, United States Code, as well as other language addressing any specific, anticipated minimization problems, such as the interception of privileged attorney-client communications, or conversations in a foreign language or code. 18 U.S.C. § 2518(5); United States v. Scott, 436 U.S. 128 (1978) (minimization efforts must be objectively reasonable); United States v. London, 66 F.3d 1227 (1st Cir. 1995) (three factors should be considered to determine whether minimization was reasonable: 1) the nature and complexity of suspected crimes; 2) the government's efforts to minimize; and 3) the degree of supervision by the judge), cert. denied, 116 S. Ct. 1542 (1996).

If any of the named subjects are facing pending state or federal criminal charges, these persons and the nature of their pending charges should be identified in the affidavit, and both the minimization language in the affidavit and the instructions given to the monitoring agents should contain cautionary language regarding the interception of privileged attorney-client conversations. The essential elements of the attorney-client privilege are: 1) the client sought legal advice; 2) the advice was sought from an attorney acting in his professional capacity;

3) the communication between the attorney and the client was for the purpose of seeking legal advice; and 4) the communication was made in confidence. United States v. Gotti, 771 F. Supp. 535 (E.D.N.Y. 1991). The privilege is not available if a non-privileged third party is present during the conversation, or if the content of the communication is disclosed to such a third party, or if the communication was made for the purpose of committing a crime. Gotti, supra.

If a monitor intercepts a privileged attorney-client conversation, the monitor should make a notation of that conversation on the log and notify the supervising attorney, who should advise the judge. The tape of the conversation should be sealed and no disclosure of that conversation should be made to other investigative officers. See United States v. Noriega, 764 F. Supp. 1480 (S.D. Fla. 1991) (tapes were first screened by an agent unconnected with the case; if the tapes contained attorney-client communications, the agent was to seal the tapes immediately and segregate them from the rest; if only part of the tape contained attorney-client conversations, then a sanitized copy of it would be provided to the case agents and prosecuting attorneys). If the interception of attorney-client conversations is inadvertent and the government acted in good faith, then only the privileged conversations will be suppressed. See also United States v. Ozar, 50 F.3d 1440 (8th Cir.), cert. denied, 116 S. Ct. 193 (1995).

If any of the named subjects speak a foreign language or converse in code, the statute permits after-the-fact minimization of wire and oral communications when an expert in that code or foreign language is not reasonably available to minimize the conversations contemporaneously with their interception. In either event, the minimization must be accomplished as soon as practicable after the interception. 18 U.S.C. § 2518(5). Such after-the-fact minimization can be accomplished by an interpreter who listens to all of the communications after they have been recorded and then gives only the pertinent communications to the agent. See United States v. David, 940 F.2d 722 (1st Cir.) ("by translating only the portions of the tapes that seemed relevant, the government's actions comported with the expectations of Congress"), cert. denied, 502 U.S. 989 (1991); United States v. Gambino, 734 F. Supp. 1084 (S.D.N.Y. 1990) (an interpreter need not be on constant duty; efforts to hire more translators had failed).

After-the-fact minimization is a necessity for the interception of electronic communications over a digital-display pager or an electronic facsimile machine. In such cases, all communications are recorded and then examined by a monitoring agent and/or a supervising attorney to determine their relevance to the investigation. Disclosure is then limited to those communications by the subjects or their confederates that are

criminal in nature. See United States v. Tutino, 883 F.2d 1125 (2d Cir. 1989) ("because it is impossible to tell from the clone beeper whether a conversation even took place, much less the content of any conversation that might have taken place, traditional minimization requirements do not apply"), cert. denied, 493 U.S. 1081 (1990).

Finally, when communications are intercepted that relate to any offense not enumerated in the authorization order, the monitoring agent should report it immediately to the AUSA, who should notify the court at the earliest opportunity. Approval by the issuing judge should be sought for the continued interception of such conversations. 18 U.S.C. § 2517(5).

h. When the request is to intercept a cellular or otherwise mobile telephone (i.e., a car, or otherwise portable, telephone) or a portable paging device, or to install a microphone in an automobile, the affidavit should contain a statement that, pursuant to 18 U.S.C. § 2518(3), the interceptions may occur not only within the territorial jurisdiction of the court in which the application is made, but also outside that jurisdiction (but within the United States). Because these devices are easily transported across district lines, this language should be used if there is any indication that the target telephone, paging device, or vehicle will be taken outside the jurisdiction of the court issuing the electronic surveillance order. The order should specifically authorize such extra-jurisdictional interceptions, and should be sought in the jurisdiction having the strongest investigative nexus to the object in which the monitoring device is installed. See United States v. Ramirez, 112 F.3d 849 (7th Cir. 1997).

3. The Order

The authorizing language of the order should mirror the requesting language of the application and affidavit, and comply with 18 U.S.C. § 2518(3), (4), and (5). In short, the order must state that there is probable cause to believe that the named violators are committing particular Title III predicate offenses (or, in the case of electronic communications, any federal felony); that the named interceptees have used, are using, and/or will use the target facility or premises (described with particularity) in furtherance thereof; that particular communications concerning the predicate offenses will be obtained through the requested interception; and that normal investigative techniques have been tried and have failed, or are reasonably unlikely to succeed if tried, or are too dangerous to employ. The court will then order that the agents of the investigative agency are authorized to intercept the communications over the described facility or at the described premises for a specific length of time, and that the interception must be conducted in such a way as to minimize the interception of communications not

otherwise subject to interception. The court may also mandate that the government make periodic progress reports, pursuant to 18 U.S.C. § 2518(6). In the case of a roving interception, the court must make a specific finding that the requirements of 18 U.S.C. § 2518(11) have been demonstrated adequately. Any other special circumstances, such as extra-jurisdictional interception in the case of mobile interception devices (pursuant to 18 U.S.C. § 2518(3)) or surreptitious entry should also be authorized specifically in the order. An order to seal all of the pleadings should also be sought at this time. 18 U.S.C. § 2518(8)(b).

The government should also prepare for the court a technical assistance order to be served on the communication service provider. 18 U.S.C. §§ 2511(2)(a)(ii) and 2518(4). This is a redacted order that requires the service provider to assist the agents in effecting the electronic surveillance.

IV. ELECTRONIC COMMUNICATIONS

1. Coverage under Title III

One of the primary changes effected by ECPA was the addition of electronic communications to the types of communications, in addition to oral and wire, whose interception is regulated by Title III. An "electronic communication" is one in which the human voice is not used in any part of the communication. 18 U.S.C. § 2510(12). The types of electronic communications that are most commonly the subject of Title III applications are those occurring over digital-display paging devices and electronic facsimile machines. Interception over these devices is usually accomplished through the use of duplicate or "clone" pagers and facsimile machines, and applications for these types of interceptions must comply with the requirements set forth in section 2518. Unlike applications to intercept oral or wire communications, section 2516(3) provides that any attorney for the government may authorize an application to be made to intercept electronic communications. By agreement with Congress, however, prior Department approval is required for most applications to conduct interceptions of electronic communications. On February 1, 1991, an exception was made for electronic communications intercepted over digital-display pagers; applications involving digital-display pagers may be authorized by an Assistant United States Attorney. This exception applies only to interceptions involving electronic communications to digital-display pagers, the most commonly targeted type of electronic communication. Department approval is still required as a prerequisite to filing an application for an interception order targeting any other form of electronic communication (e.g., facsimile transmissions, electronic mail, and computer transmissions).

2. Stored Electronic Communications - 18 U.S.C. § 2703

In addition to the changes to numerous provisions of Title III, ECPA also defined and regulated government access to various new forms of electronic communications, including stored electronic communications and transactional records.

a. Under 18 U.S.C. § 2703(a), the government may require a service provider to disclose the contents of an electronic communication that is in electronic storage¹ in an electronic communications system² for one hundred and eighty days or less, only pursuant to a search warrant. (As defined in 18 U.S.C. § 2510(8), "'contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.") If the information has been in electronic storage for more than one hundred and eighty days, disclosure may be required by a search warrant (without prior notice to the subscriber), a court order sought pursuant to section 2703(d) (with prior notice to the subscriber, requirements for this order are summarized below), or an administrative, grand jury, or trial subpoena (with prior notice to the subscriber). Delayed notice to the subscriber may be sought under section 2705.

Under section 2703(b), the government may obtain the contents of any electronic communication held in a remote

¹ "Electronic storage" is defined in 18 U.S.C. § 2510(17) as: "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." To illustrate "incidental to ... transmission," consider the example of electronic mail. If electronic mail has been sent but not opened by the intended recipient, then it is in "electronic storage ... incidental to ... transmission." Once the electronic mail has been opened by the recipient, it can be argued that the electronic mail is no longer in electronic storage incidental to transmission.

² An "electronic communication service provides its users the ability to send or receive wire or electronic communications." S. Rep. No. 541, 99th Cong., 2d Sess. 14 (1986). Examples of electronic communication services would be telephone companies (such as Bell Atlantic) and electronic mail companies (such as America On Line). *Id.* Bell Atlantic serves as an electronic communication service when it facilitates the placement of telephone calls, and America On Line does, as well, when it transmits electronic mail from the sender to the recipient.

computing service³ by way of a search warrant, an administrative, grand jury, or trial subpoena, or a court order authorized by section 2703(d), with a request seeking delayed notice to the subscriber/customer pursuant to section 2705. See Steve Jackson Games, Incorporated v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994) (upheld use of search warrant to seize stored email on computer). The following language from the appellate court in Steve Jackson Games, however, has contributed to the confusion concerning access to stored wire communications:

Appellants overemphasize the significance of this reference [§ 2701(c)(3)] to § 2518...it is clear that Congress intended to treat wire communications differently from electronic communications. Access to stored electronic communications may be obtained pursuant to a search warrant, 18 U.S.C. § 2703; but access to stored wire communications requires a court order pursuant to § 2518. Because § 2701 covers both stored wire and electronic communications, it was necessary in subsection (c) [of § 2701] to refer to the different provisions authorizing access to each.

Id. at 464. But see United States v. Moriarty, 962 F. Supp. 217 (D. Mass. 1997) ("only the interception of voice mail while in transmission, like a wiretap on a telephone in use, can amount to a violation of Section 2511").

b. Under 18 U.S.C. § 2703(c)(1)(C), the government may obtain from an electronic communication service provider a subscriber's or customer's name, address, telephone toll billing records (this includes local and long distance cellular air-time records, see In re Matter of Grand Jury Subpoenas to Southwestern Bell Mobile Systems, Inc., 894 F. Supp. 355 (W.D. Mo. 1995)), telephone number, or other subscriber number or identity, length of service, and types of services utilized, by administrative subpoena, or a grand jury or trial subpoena. If subpoena authority is not available, the government may obtain the

³ As described in H. Rep. No. 647, 99th Cong., 2d Sess. 23 (1986), remote computer services allow "persons [to] use the facilities of these services to process and store their own data." The House Report further explains that "[a] subscriber or customer to a remote computing service transmits records to a third party, a service provider, for the purpose of computer processing. This processing can be done with the customer or subscriber using the facilities of the remote computing service in essentially a time-sharing arrangement, or it can be accomplished by the service provider on the basis of information supplied by the subscriber or customer." Id. America On Line (AOL) would function as a remote computing service when the recipient of an electronic mail transmission decides to save the transmission on AOL's system.

information pursuant to a search warrant, a court order under 18 U.S.C. § 2703(d), or the consent of the subscriber or customer. The requirements for obtaining a section 2703(d) court order must be met even if the government seeks the court order only to obtain subscriber and telephone information. Those requirements are that the government must offer "... specific and articulable facts showing that there are reasonable grounds to believe that ... the records or other information sought are relevant and material to an ongoing criminal investigation." Id.

c. Pursuant to 18 U.S.C. § 2703(f) (Supp. 1996), a service provider or remote computing service, upon the request of a governmental entity, must preserve records and other evidence in its possession pending the issuance of a court order or other process.

For additional information concerning stored electronic communications, contact the Computer Crime and Intellectual Property Section at (202) 514-1026.

V. EXTENSION AND SPINOFF APPLICATIONS

1. Extension Applications

Applications to continue previously authorized electronic surveillance for an additional period, usually another thirty days, may be made at or near the expiration of the previous thirty-day order. (If, for scheduling reasons, an extension application must be filed before the end of an ongoing thirty-day period, the new thirty-day period is calculated from the date of the extension order.) As long as the investigation is continuing, subsequent applications to continue interceptions over the same facility or at the same location, and involving substantially the same subjects and offenses are considered extensions. See United States v. Plescia, 48 F.3d 1452 (7th Cir.), cert. denied, 116 S. Ct. 114 (1995); United States v. Carson, 969 F.2d 1480 (3d Cir. 1992). As noted above, extension applications require Department authorization, but are reviewed only by the ESU and not the investigative agency. An exception occurs when the electronic surveillance has been inactive for more than thirty days; in these instances, the Department requires that a new memorandum requesting renewed electronic surveillance be submitted by the head of the investigative agency.

The tapes should be sealed at the end of each interception period, especially if the investigation is lengthy and definitely whenever there is any time gap between extensions. While the statute requires the tapes to be sealed at the "expiration of the period of the order, or extensions thereof," the appellate courts have differed on the amount of time that may elapse between orders before the new order is no longer considered an extension,

and, thus, necessitating sealing under the statute. If there is a sealing delay, a good reason for the delay must be provided and a showing made that the defendant was not prejudiced by the failure to seal in a timely fashion. See United States v. Oieda-Rios, 495 U.S. 257 (1990) (Title 18, United States Code, Section 2518(8)(a) requires the court to presume prejudice if the sealing requirements are not met).

An extension affidavit follows the same format and carries the same statutory requirements as does the affidavit that supported the original application. 18 U.S.C. § 2518(5). The primary difference is in the probable cause section, which must focus on the results obtained (or lack thereof) during the most recent interception period, including any new information regarding the subjects' recent use of the targeted facilities or premises. 18 U.S.C. § 2518(1)(f). The affidavit should incorporate by reference the original and all previous extension applications, and then discuss in a paragraph or two the progress of the investigation to date and summarize new information obtained during the past thirty days. If no relevant interceptions were made during the previous period, a sufficient explanation must be provided to the court (for example, technical or installation problems with monitoring equipment, or the physical absence of the subject during all or part of the interception period), along with a reasonable, factually based explanation of why the problems are expected to be rectified during the next thirty days. Id. A sampling of recent interceptions sufficient to establish probable cause that the subjects are continuing to use the targeted facilities or location in furtherance of the stated offenses should then be described. The affidavit should not contain verbatim transcripts or a series of pieced-together progress reports; rather, selected and paraphrased or highlighted portions of a few key, criminal conversations should be set forth, along with an explanation, if necessary, of the context in which the conversations were spoken, and the affiant's opinion (based on his/her training and experience) of their meaning if they are in code or are otherwise unclear. The excerpted conversations should reflect results obtained over the bulk of the thirty-day period, and not consist solely of interceptions obtained, for example, during the first ten days.

Other changes from the original application will be in the "Need for Interception and Alternative Investigative Techniques" section, which should state that the facts set forth in the original affidavit regarding the exhaustion of alternative investigative techniques are continuing, citing examples of what additional efforts have been made during the preceding interception period, and explaining why the electronic surveillance conducted thus far has been insufficient to meet the goals of the investigation. See United States v. Castillo-Garcia, 920 F. Supp. 1537 (D. Colo. 1996) (alternative

investigative techniques section should have been updated and justified in every subsequent extension affidavit), modified, 117 F.3d 1179 (10th Cir. 1997). It is also frequently necessary to add or delete subjects and offenses due to new information learned from the interceptions. If any additional subjects are added, an ELSUR check needs to be done for their names.

Finally, Title III does not limit the number of extension affidavits that may be filed. United States v. Vazquez, 605 F.2d 1269 (2d Cir.), cert. denied, 444 U.S. 981 (1979); United States v. Ruggiero, 824 F. Supp. 379 (S.D.N.Y. 1993). If the objective of the intercept is to determine a conspiracy's scope and to identify its participants, more extensive surveillance may be justified. United States v. Nguyen, 46 F.3d 781 (8th Cir. 1995); United States v. Earls, 42 F.3d 1321 (10th Cir. 1994), cert. denied, 514 U.S. 1085 (1995). In addition, interceptions need not terminate because some targets have been arrested. United States v. Wong, 40 F.3d 1347 (2d Cir. 1994), cert. denied, 116 S. Ct. 190 (1995).

The ESU can usually review and process these applications in three to four days, depending upon the caseload of the attorney assigned to the case. If it is important that the electronic surveillance not be interrupted between orders, the extension request should be submitted to the ESU with sufficient lead time.

2. Spinoff Applications

As stated above, new applications arising from the same investigation to conduct electronic surveillance over additional facilities are considered original requests, even though the same subjects are targeted, and are reviewed and processed by both the ESU and the investigative agency as such. A new facility is one which, in the case of landline telephones, is carried over a different cable, pair, and binding posts, or, in the case of cellular telephones, over an instrument bearing a different electronic serial number and telephone number than that of the originally authorized facility. Thus, for example, a targeted landline telephone that is given a new telephone number during an interception period, but which maintains the same location (the same cable, pair, and binding posts) is not considered a spinoff, and applications for additional thirty-day interception periods are extensions of the original authorization. If this situation occurs and the subject of the electronic surveillance obtains a new number for the telephone during the course of the monitoring, the court should be notified.

As with extension requests, prior affidavits in the same investigation may be incorporated by reference, obviating the need to set forth anew all of the facts that established the original probable cause; the probable cause section in the spinoff application should focus on the newly targeted facility

or location, and any additional subjects. As noted above, if new subjects are added, an ELSUR check must be done for their names.

A spinoff application may not, however, merely incorporate by reference the "Need for Interception and Exhaustion of Alternative Techniques" section of the original affidavit. This section must address the facts as they apply to the spinoff application. See United States v. Santora, 600 F.2d 1317 (9th Cir. 1979) (evidence was suppressed because the spinoff affidavit incorporated by reference the original affidavit's showing of inadequacy of normal investigative procedures; spinoff affidavits require a showing of the difficulties of employing normal investigative techniques with regard to the new telephone, premises and subjects) and United States v. Castillo-Garcia, 920 F. Supp. 1537 (D. Colo. 1996), modified, 117 F.3d 1179 (10th Cir. 1997).

The minimization language of the original affidavit should also be reviewed to ensure that it comports with any new facts particular to the new facility or location.

VI. ROVING INTERCEPTIONS

ECPA established the "roving" provisions of Title III. See 18 U.S.C. § 2518(11), (12). These provisions permit the interception of oral, wire, or electronic communications of named subjects without requiring that a specific facility or premises be identified in advance of the authorization. The roving provisions are intended to be used infrequently, and only when the required elements have been fulfilled clearly. Authorization for a roving interception must be granted by a Department of Justice official at the Assistant Attorney General or Acting Assistant Attorney General level or higher.

In a roving interception, the requirements of 18 U.S.C. § 2518(1)(b)(ii), necessitating a particular description of the nature and location of the facilities from which or the place where the communications are to be intercepted, may be waived when, in the case of an oral interception, identification of a specific premises prior to court authorization is not practical; and in the case of a wire or an electronic interception, when a particular subject is using various and changing facilities for the purpose of thwarting electronic surveillance. In each circumstance, the subject who is the target of a roving interception must be identified at the time the application is made and only those conversations in which the subject is a participant may be intercepted. Once the named subject is no longer a party to the conversation, the interception must cease, even though the conversation may be criminal in nature. In practice, it is helpful to remember that the authorization attaches to a specific subject, rather than to a particular facility or location.

Monitoring agents must, however, identify a specific telephone or location before the interception begins (18 U.S.C. § 2518(12)); that is, monitoring may not begin over telephones or within locations suspected of being used by a specific subject until the monitoring agent ascertains that the subject is, in fact, using that particular facility or location. While it is not necessary to notify the court before monitoring begins, it should be done as soon as practicable. The ESU takes the position that if physical surveillance is not possible, spot monitoring may be employed to meet the ascertainment requirement of section 2518(12) before "actual interception" begins under a roving interception order.

1. Roving Oral Interception

In the case of a roving oral interception, the application must establish, and the order must specifically find, that probable cause exists that a particular subject is committing a Title III predicate offense at locations that are not practical to specify. 18 U.S.C. § 2518(11)(a)(ii); United States v. Bianco, 998 F.2d 1112 (2d Cir. 1993), cert. denied, 511 U.S. 1069 (1994); United States v. Orena, 883 F. Supp. 849 (E.D.N.Y. 1995).

The impracticality element may be established by informant information showing that the named subject changes meeting places frequently and with little or no warning, usually in order to avoid law enforcement surveillance, combined with a pattern of physical surveillance over a period of weeks confirming that the subject does, in fact, meet at changing locations with little or no advance warning sufficient to permit prior identification of a targeted premises. While the amount and type of evidence available will vary with the particular circumstances of each case, it is essential in all cases that enough factual background information be provided to support the court's finding that it is impractical to specify a particular location at the time the application is filed.

Because of the technical difficulties inherent in obtaining interceptions pursuant to a roving oral authorization, it is wise to check with the field and technical agents before time and resources are expended doing the preliminary fieldwork and drafting the affidavit. The statutory requirements for obtaining a roving oral interception order make actual execution of the order difficult: unless the roving oral interception is done in conjunction with an ongoing wiretap or with the benefit of up-to-the-minute information from an informant or undercover agent concerning the location of an impending meeting, it is usually technically impossible to effect the interceptions, because there is no time to install monitoring equipment before the meeting occurs. Sufficient advance notice of a specific location, however, argues in favor of targeting a particular location through a regular electronic surveillance order rather

than using the roving provision. Thus, field agents should be required to present a practical and reasonably workable plan for installing the listening device prior to requesting a roving oral interception.

2. Roving Wire or Electronic Interception

In the case of a roving wire or electronic interception, 18 U.S.C. § 2518(11)(b)(ii) requires a showing that a named subject uses various and changing facilities to thwart electronic surveillance. This can be shown through informant information concerning the subject's fear of wiretaps and his intention to use public telephones or cellular telephones to conduct criminal business, combined with physical surveillance and telephone records from public or cellular telephones reflecting calls by the subject to known or suspected criminal associates. It is inadequate merely to allege that the subject has been observed using several pay or cellular telephones and, therefore, must be doing so in an attempt to thwart electronic surveillance. A sufficient factual basis must be established to permit the court to make the required finding that the subject has demonstrated a clear intent (optimally through a pattern covering a period of weeks) to use various facilities in order to thwart electronic interception. See United States v. Gaytan, 74 F.3d 545 (5th Cir.), cert. denied, 117 S. Ct. 77 (1996); United States v. Petti, 973 F.2d 1441 (9th Cir. 1992), cert. denied, 507 U.S. 1035 (1993); United States v. Villegas, 1993 WL 535013 (S.D.N.Y. Dec. 22, 1993) (unreported). Although the statute does not distinguish between public, cellular, and residential telephones, it is the Department's policy that, except in rare occasions involving the rapidly changing use of telephones located in hotel rooms or restaurants, only cellular or public pay telephones may be targeted in a roving wiretap.

While the statute does not address the jurisdictional restrictions of a roving interception, the legislative history suggests, and Department policy concurs, that roving interception authorization is not transjurisdictional; orders must be obtained in each jurisdiction in which roving interceptions are to be conducted. However, in cases involving mobile cellular telephones or vehicles that cross jurisdictional lines, 18 U.S.C. § 2518(3), which permits extra-jurisdictional orders, would apply.

VII. EMERGENCY PROCEDURES

1. Title III Interceptions

Title 18, United States Code, Section 2518(7), permits the Attorney General (AG), the Deputy Attorney General (DAG), or the Associate Attorney General (Assoc. AG) to specially designate any

investigative or law enforcement officer to determine whether an emergency situation exists that requires the interception of wire, oral, or electronic communications pursuant to Title III before a court order can, with due diligence, be obtained. The statute defines an emergency situation as one involving an immediate danger of death or serious injury to any person, conspiratorial activities threatening the national security interest, or conspiratorial activities characteristic of organized crime. 18 U.S.C. § 2518(7). In all but the most unusual circumstances, the only situations likely to constitute an emergency are those involving an imminent threat to life, e.g., a kidnapping or hostage taking, or imminent terrorist activity. See Nabozny v. Marshall, 781 F.2d 83 (6th Cir.) (kidnapping and extortion scenario constituted an emergency situation), cert. denied, 476 U.S. 1161 (1986); United States v. Crouch, 666 F. Supp. 1414 (N.D. Cal. 1987) (wiretap evidence suppressed because there was no imminent threat of death or serious injury). Because the Federal Bureau of Investigation has jurisdiction over these offenses, the Bureau will likely be the requesting agency in an emergency.

The Criminal Division's emergency procedures require that before the requesting agency contacts the AG, the DAG, or the Assoc. AG, oral approval to make the request must first be obtained from the Assistant Attorney General (AAG) or a Deputy Assistant Attorney General (DAAG) of the Criminal Division. This approval is facilitated by the ESU, which is the initial contact for the requesting United States Attorney's Office and the agency. In practice, the emergency procedures are initiated when the AUSA in charge of the case contacts an ESU attorney. At the same time, the field agents contact their agency headquarters personnel. After discussions with both the AUSA and an agency headquarters representative, the ESU attorney, in consultation with the OEO Director or an Associate Director, determines whether the statutory requirements have been met. Both the ESU and the agency's headquarters must agree that an emergency situation and the means to implement the requested electronic surveillance exist. The ESU attorney then briefs the AAG or a DAAG and obtains oral authorization on behalf of the Criminal Division. The ESU attorney notifies the agency representative that the Division has approved the seeking of an emergency authorization. The appropriate agency representative (usually the Director or Deputy Director of the FBI) then contacts the AG, the DAG, or the Assoc. AG and seeks permission to make a determination that an emergency situation exists as defined in the statute.

Once the AG, the DAG, or the Assoc. AG authorizes the law enforcement agency to make the determination whether to proceed with the emergency Title III, the government then has forty-eight hours (including weekends and holidays) from the time the authorization was obtained to apply for a court order approving the interception. The package submitted to the court will

consist of the AUSA's application, the affidavit, and a proposed order. (This package must be reviewed by the ESU before it is submitted to the court.) The affidavit in support of the government's after-the-fact application to the court for an order approving the emergency interception must contain only those facts known to the AG, the DAG, or the Assoc. AG at the time the emergency interception was approved. The application must be accompanied by a written verification from the requesting agency noting the date and time of the emergency authorization. The government may request, at the time it files for court-authorization for the emergency, court-authorization to continue the interception beyond the initial forty-eight hour period. If continued authorization is sought at the same time, one affidavit may be submitted in support of the emergency application and the extension application, but the affidavit must clearly indicate which information was communicated to the AG, the DAG, or the Assoc. AG at the time the emergency interception was approved and which information was developed thereafter. Two separate applications and proposed orders (one set for the emergency and one set for the extension) should be submitted to the court. If the government seeks continued authorization, that application must be reviewed by the ESU and approved by the Criminal Division like any other Title III request would.

2. Pen Register/Trap and Trace Devices

Title 18, United States Code, Section 3125 permits the AG, the DAG, the Assoc. AG, any AAG, any Acting AAG, or any DAAG to specially designate any investigative or law enforcement officer to determine whether an emergency situation exists requiring the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained. An emergency situation under this section exists if it involves the immediate danger of death or serious injury to any person, or conspiratorial activities characteristic of organized crime. Unlike the Title III emergency provision, under 18 U.S.C. § 3125, a situation involving conspiratorial activities threatening national security does not, in itself, constitute an emergency. The government has forty-eight hours after the installation has occurred to obtain a court order in accordance with section 3123 approving the installation or use of the pen register/trap and trace device. Failure to obtain a court order within this forty-eight-hour period shall constitute a violation of the pen register/trap and trace chapter.

As with an emergency Title III, the AUSA in charge of the case should contact the ESU to request an emergency pen register or trap and trace. After discussions with the AUSA, the ESU attorney, in consultation with the OEO Director or an Associate Director, determines whether the statutory requirements have been met. If so, the ESU attorney will contact the appropriate Criminal Division official and obtain authorization to proceed.

Once that approval has been obtained, the ESU attorney will contact the AUSA and advise that the emergency use has been approved, and that the law enforcement agency may proceed with the installation and use of the pen register/trap and trace. The ESU attorney will send a verification memorandum, signed by the authorizing official, to the AUSA. The AUSA should submit this authorization memorandum with the application for the court order approving the emergency use.

3. How to Contact the ESU

If an emergency situation arises after regular business hours, an ESU attorney may be reached through the Department of Justice Command Center at (202) 514-5000. During regular business hours, the ESU may be reached at (202) 514-6809; fax - (202) 616-2010.

VIII. PROGRESS REPORTS

Title 18, United States Code, Section 2518(6) provides for periodic progress reports to be made at the judge's discretion. These are generally made at five-, seven-, or ten-day intervals, and should contain enough (summarized) excerpts from intercepted conversations to establish continuing probable cause and need for the surveillance. Any new investigative information pertinent to the electronic surveillance, such as newly identified subjects or the addition of new violations, should be brought to the court's attention in the progress reports, and then be included in the next extension request. See generally, United States v. Van Horn, 789 F.2d 1492 (11th Cir.), cert. denied, 479 U.S. 854 (1986); In re De Monte, 674 F.2d 1169 (7th Cir. 1982); United States v. Plescia, 773 F. Supp. 1068 (N.D. Ill. 1991).

IX. SEALING

1. Overview

Title 18, United States Code, Section 2518(8)(a) requires that the tape recordings of the intercepted conversations be sealed "[i]mmediately upon the expiration of the period of the order, or extensions thereof." The purpose of the sealing requirement is to preserve the integrity of the electronic surveillance evidence. Section 2518(8)(a) contains an explicit exclusionary remedy for failure to comply with the sealing requirement: "[t]he presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of any...[electronic surveillance] evidence ... under subsection (3) of section 2517." This provision requires that the government explain not only why it failed to seal or why a delay in sealing occurred, but also why the failure or delay is excusable. See United States v. Ojeda-Rios, 495 U.S. 257 (1990); United States

v. Carson, 52 F.3d 1173 (2d Cir. 1995), cert. denied, 116 S. Ct. 934 (1996).

2. When to Seal

As noted above, 18 U.S.C. § 2518(8)(a) requires that the tape recordings of the intercepted conversations be sealed "[i]mmediately upon the expiration of the period of the order, or extensions thereof." If the government does not seek an extension of the original order, then the tapes of the intercepted conversations must be sealed immediately upon the expiration of the original order. If an extension or several extension orders are obtained, then the tapes of the intercepted conversations must be sealed upon the expiration of the last extension order. The definition of an extension order is construed very narrowly, and applies only "whe[n] the surveillance involves the same telephone, the same premises, the same crimes, and substantially the same persons" as the original order. United States v. Gallo, 863 F.2d 185 (2d Cir. 1988), cert. denied, 489 U.S. 1083 (1989); United States v. Scafidi, 564 F.2d 633 (2d Cir. 1977), cert. denied, 436 U.S. 903 (1978).

When caused by administrative difficulties, a brief hiatus between the expiration of an order and the extension will not prevent the extension from being deemed an "extension" within the meaning of section 2518(8)(a). Thus, the obligation to seal will not arise until the termination of the final extension order. See United States v. Plescia, 48 F.3d 1452 (7th Cir. 1995), cert. denied, 116 S. Ct. 114 (1995); United States v. Carson, 969 F.2d 1480 (3d Cir. 1992); United States v. Nersesian, 824 F.2d 1294 (2d Cir.), cert. denied, 484 U.S. 957 (1987). Despite the statutory language and the case law, the Department recommends that the AUSA seal the tapes at the end of each extension order to ensure the integrity of each month's interceptions. It is better to seal immediately every thirty days than to have to explain months, or even years, later why the tapes were not sealed during some minimal gaps in the interception period, and hope that the court will find that the explanation is satisfactory (even when it is clear that the tapes have not been altered).

A spinoff order targeting a different facility is not an extension, even though it involves the same subjects or investigation. Accordingly, those tape recordings should be sealed as soon as that interception order expires when no extension is contemplated. Each spinoff should likewise be compartmentalized.

3. Sealing Delays

Numerous court opinions issued in the Second Circuit have held that a sealing delay of more than two days requires the government to provide a satisfactory explanation for violating

the "immediate" sealing requirement of section 2518(8)(a). See United States v. Pitera, 5 F.3d 624 (2d Cir. 1993), cert. denied, 510 U.S. 1131 (1994); United States v. Ardito, 782 F.2d 358 (2d Cir.), cert. denied, 475 U.S. 1141 (1986); United States v. Orena, 883 F. Supp. 849 (E.D.N.Y. 1995); United States v. Burford, 755 F. Supp. 607 (S.D.N.Y. 1991); United States v. Casso, 843 F. Supp. 829 (E.D.N.Y. 1994).

When the issuing judge is unavailable, that circumstance will likely constitute a satisfactory explanation for a slightly extended sealing delay. United States v. Maxwell, 25 F.3d 1389 (8th Cir.) (judge scheduled the sealing for seven days after termination), cert. denied, 513 U.S. 1031 (1994); United States v. Pedroni, 958 F.2d 262 (9th Cir. 1992) (issuing judge was out of town for several days after the tapes were ready for sealing); United States v. Fury, 554 F.2d 522 (2d Cir.) (six-day delay because issuing judge was on vacation and unavailable), cert. denied, 433 U.S. 910 (1977); United States v. Blanco, 1994 WL 695396 (N.D. Cal. December 8, 1994) (unreported) (tapes were ready for sealing within three days of termination, but due to continuing unavailability of the issuing judge and other district judges, a magistrate granted the government's request for a sealing order sixteen days after termination of the interception, and upon return to the district, the issuing judge granted the government's application for an order ratifying the magistrate's sealing order).

The failure to seal immediately because of unexpected resource or personnel shortages has been deemed a "satisfactory explanation." Pedroni, supra (agent in charge of case took time to interview two potential witnesses who became available at the time when the tapes were being prepared for sealing); United States v. Rodriguez, 786 F.2d 472 (2d Cir. 1986) (fourteen-day delay because supervising attorney occupied with another trial); United States v. Massino, 784 F.2d 153 (2d Cir. 1986) (fifteen-day delay because government diverted personnel to investigate leak threatening investigation); United States v. Scafidi, 564 F.2d 633 (2d Cir. 1977) (seven-day delay because prosecutor preoccupied with upcoming trial). Compare United States v. Quintero, 38 F.3d 1317 (3d Cir. 1994) (because the AUSA's caseload was foreseeable, the tapes should have been sealed immediately), cert. denied, 513 U.S. 1195 (1995).

A government attorney's objectively reasonable "mistake of law" may be a satisfactory explanation for a sealing delay. United States v. Wilkinson, 53 F.3d 757 (6th Cir. 1995) ("good faith" misunderstanding of court order); United States v. Vastola, 25 F.3d 164 (3d Cir.) (affirmed district court's finding on remand that AUSA's combined reading of the law and her reliance on the opinions of more experienced colleagues on the sealing issue was minimally sufficient to meet the standards of a reasonably prudent attorney), cert. denied, 513 U.S. 1015 (1994); United States v. Carson, 969 F.2d 1480 (3d Cir. 1992) (even if a

government attorney's legal conclusion was found to be unreasonable, the explanation for the delay would still be an objectively reasonable "mistake of law" if the government could show that its attorney had adequately researched the law or had otherwise acted reasonably). Notwithstanding the overall favorable case law, the ESU still stresses the importance of sealing every thirty days to obviate the issue at trial and on appeal.

4. How to Seal/Custody of the Tapes

Sealing is accomplished by making the original recordings of the intercepted conversations available to the judge who issued the interception order. In United States v. Abraham, 541 F.2d 624 (6th Cir. 1976), the statutory sealing requirements were met when the government attorney advised the district judge that the tapes were available for inspection at the time he presented motions for orders sealing them; it was not necessary that the recordings be sealed in the judge's presence. Typically, however, the AUSA and the case agent will deliver the tapes to the judge, who will then physically seal the box containing the tapes, initialing and dating the evidence tape. The judge will then issue a sealing order and determine where the tapes are to be kept. The judge will usually order that the investigative agency retain custody of the sealed tape recordings.

5. Suppression for Failure to Seal Properly

Failure to seal the tapes properly or to offer a satisfactory explanation for a sealing delay will likely result in suppression of the evidence. Compare United States v. Carson, 969 F.2d 1480 (3d Cir. 1992) (thirty-four-day delay in sealing for purpose of audio enhancement was not a satisfactory explanation; government should have sealed the tapes and sought order to unseal for purpose of enhancement) with United States v. Fiumara, 727 F.2d 209 (2d Cir.) (unsealing order authorized the government to unseal the tapes to the limited extent necessary to duplicate, disclose, and otherwise make use of them; a private audio expert's "custody of the tapes for purposes of enhancement and duplication" was consistent with this order), cert. denied, 466 U.S. 951 (1984). See also United States v. Feiste, 961 F.2d 1349 (8th Cir. 1992) (thirty-one-day delay).

6. Resealing

Once the trial has ended and the need for the electronic surveillance tapes has concluded, the original tapes should be resealed in order to preserve their integrity for use in other proceedings. Even after surveillance tapes have been used in one judicial proceeding, they may not be admitted into evidence in another without a judicial seal "or a satisfactory explanation for the absence thereof." 18 U.S.C. § 2518(8)(a). See United States v. Long, 917 F.2d 691 (2d Cir. 1990); United States v.

Scopo, 861 F.2d 339 (2d Cir. 1988), cert. denied, 490 U.S. 1022 (1989).

X. INVENTORY NOTICE

Title 18, United States Code, Section 2518(8)(d) requires an inventory notice to be served on persons named in the order, and "...other such parties to intercepted communications as the judge may determine ... is in the interest of justice ..." within a reasonable time, but not later than 90 days after the end of the last extension order. The government has an obligation to categorize those persons whose communications were intercepted so that the judge may make a reasoned determination about whether they will receive inventory notice. United States v. Donovan, 429 U.S. 413 (1977); United States v. Alfonso, 552 F.2d 605 (5th Cir. 1977), cert. denied, 434 U.S. 857 (1977); United States v. Chun, 503 F.2d 533 (9th Cir. 1974). The inventory should state that an order or application was entered, the date it was entered and the period of authorized interceptions, or the denial of interception, as well as whether communications were intercepted. Upon a showing of good cause (e.g., impairment of an ongoing investigation), the court may delay service of inventory notice.

Absent a showing of bad faith or actual prejudice, the failure to serve a formal inventory notice under section 2518(8)(d) does not justify suppression. Donovan, supra; United States v. DeJesus, 887 F.2d 114 (6th Cir. 1989); United States v. Davis, 882 F.2d 1334 (8th Cir. 1989), cert. denied, 494 U.S. 1027 (1990); United States v. Savaiano, 843 F.2d 1280 (10th Cir. 1988). Suppression will likely occur only when the statutory violation arose from a conscious decision by the federal authorities to violate the law and to prevent an individual or group of individuals from receiving the post-interception notice. United States v. Harrigan, 557 F.2d 879 (1st Cir. 1977).

XI. DISCLOSURE OF TITLE III EVIDENCE

1. 18 U.S.C. § 2517(1), (2) - Law Enforcement Use

Briefly, section 2517(1) authorizes an investigative or law enforcement officer to disclose, without prior court approval, the contents of intercepted communications to another law enforcement or investigative officer, as defined by 18 U.S.C. § 2510(7). This does not permit disclosure of the information to foreign law enforcement officials; to disclose electronic surveillance information to them, a court order must be obtained pursuant to 18 U.S.C. § 2518(8)(b), which permits the disclosure upon a showing of "good cause."

Section 2517(2) permits an investigative or law enforcement officer, without prior court approval, to use the contents of properly obtained electronic surveillance evidence to the extent that such use is appropriate to the proper performance of his

official duties. See United States v. Gerena, 869 F.2d 82 (2d Cir. 1989) (use in search warrants); United States v. C'Connell, 841 F.2d 1408 (8th Cir.) (disclosure to secretaries and intelligence analysts), cert. denied, 487 U.S. 1210 (1988); United States v. Ricco, 566 F.2d 433 (2d Cir. 1977) (to refresh recollection of a witness), cert. denied, 436 U.S. 926 (1978); United States v. Rabstein, 554 F.2d 190 (5th Cir. 1977) (for voice identification).

While it is clear from the legislative history and the case law cited above that section 2517(1), (2) allows the disclosure of Title III information for any legitimate investigative purpose associated with the development of a criminal case, the release of the information under this section for other purposes is the subject of much dispute. It has been argued successfully that section 2517(1), (2) also permits disclosure for use in various civil matters, such as forfeiture cases, congressional hearings or investigations, state bar disciplinary proceedings, and civil tax investigations. See Berg v. Michigan Attorney Grievance Commission, 49 F.3d 1188 (6th Cir. 1995) ("once conversations are lawfully intercepted, disclosure is not limited to criminal proceedings"; upholding disclosure of Title III evidence to attorney grievance commission); In re Grand Jury Proceedings, 841 F.2d 1048 (11th Cir. 1988) (House committee investigating whether impeachment proceedings are warranted falls within the definition of "investigative officer"); United States v. All Right, Title and Interest..., 830 F. Supp. 750 (S.D.N.Y. 1993) (AUSAs, whether working on criminal or civil matters, fall within section 2510(7)'s definition of an "investigative or law enforcement officer").

In any event, when in doubt about whether the disclosure or use of electronic surveillance evidence is permitted, obtain a court order pursuant to 18 U.S.C. § 2518(8)(b) authorizing the disclosure and use for "good cause." (Although section 2518(8)(b) provides for the disclosure of Title III "applications and orders," the legislative history reflects that it was also intended to apply to the disclosure of the Title III recordings themselves, as well as any related documentation. See also In re Grand Jury Proceedings, 841 F.2d 1048, 1053 n.9 (11th Cir. 1988). Thus, the Department has successfully obtained disclosure orders under section 2518(8)(b) for the release of the tapes of intercepted conversations.) The Department recommends this course of action because 18 U.S.C. § 2520 provides that a good faith reliance on a court order is a complete defense to civil and criminal actions for unauthorized disclosure of electronic surveillance information.

When disclosing and using electronic surveillance information, the government must ensure that the disclosure of the electronic surveillance information does not abridge the privacy rights of parties not charged with any crime, or jeopardize an ongoing criminal investigation. See United States

v. Dorfman, 690 F.2d 1230 (7th Cir. 1982) (disclosure to a limited audience of "professionally interested strangers" in the context of their official duties is not the equivalent to disclosure to the public; "Title III does not allow public disclosure of all lawfully obtained wiretap evidence just because a few officers are privy to its contents"). See also Certain Interested Individuals v. Pulitzer Pub., 895 F.2d 460 (8th Cir.) (pre-indictment stage of criminal case "tips the balance ... in favor of the privacy interests and against disclosure of even redacted version of the search warrant affidavits at this time"), cert. denied, 498 U.S. 880 (1990); United States v. Shenberg, 791 F. Supp. 292 (S.D. Fla. 1991) (court denied media's motion seeking access to search warrants containing Title III interceptions until their admissibility was established); State v. Gilmore, 549 N.W.2d 401 (Wis. 1996) (Wisconsin electronic surveillance disclosure provisions, which are virtually identical to 18 U.S.C. § 2517(1), (2), bar the state from including legally intercepted communications in a criminal complaint unless the complaint is filed under seal). In this regard, a bluesheet dated July 10, 1994, which appears in Title 9, Chapter 7 of the United States Attorney's Manual, recommends placing under seal Title III-related material and seeking a protective order under Fed. R. Crim. Proc. 16, asking the court to forbid defense counsel from publicly disclosing the information.

2. 18 U.S.C. § 2517(3) - Testimonial Use

Section 2517(3) allows a person, without prior court approval, to disclose electronic surveillance information, or any derivative evidence, while giving testimony under oath in any federal, state, or local proceeding. It should be noted that the prerequisite for the testimonial use of electronic surveillance evidence is the "presence of the seal ... or a satisfactory explanation for the absence thereof...." 18 U.S.C. § 2518(8)(a). See Certain Interested Individuals v. Pulitzer Pub., 895 F.2d 460 (8th Cir. 1990) (disclosure of wiretap information in a search warrant affidavit is not the testimonial disclosure contemplated in section 2517(3), even though affidavits are prepared under oath or affirmation), cert denied, 498 U.S. 880 (1990).

3. 18 U.S.C. § 2517(4) - Privileged Communications

This section merely provides: "No other privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character."

4. 18 U.S.C. § 2517(5) - Use of "Other Crimes" Evidence

Section 2517(5) pertains to the interception of conversations that relate to offenses other than those specified in the authorization order. In pertinent part, that section states: "When ... a law enforcement officer ... intercepts wire,

oral, or electronic communications relating to offenses other than those specified in the order ..., the contents thereof, and evidence derived therefrom, may be disclosed or used [for law enforcement purposes] ... or disclosed under oath in any proceeding when the "... judge finds on subsequent application that the contents were otherwise intercepted in accordance with [Title III]."

If, for example, the Title III order authorizes the interception of communications related to narcotics offenses, and during the course of the interception period, conversations concerning loansharking are overheard, section 2517(5) allows the continued interception of those conversations and their use for law enforcement purposes. The court should, however, be notified as soon as practicable that conversations about other offenses are being monitored, and the new offenses should be added to the pleadings if an extension order is obtained. By including the new offenses in the extension order, the government may use that evidence in future proceedings without having to obtain additional court-authorization later. If no extension order is obtained and the government wishes to use that evidence in a future proceeding, an order should be obtained as soon as practicable pursuant to 18 U.S.C. § 2517(5). See United States v. Barnes, 47 F.3d 963 (8th Cir. 1995) ("judicial approval ... might retroactively be granted pursuant to § 2517(5) upon ... a showing" that the communications concerning the unauthorized offenses were incidentally intercepted); United States v. Shields, 999 F.2d 1090 (7th Cir. 1993) (same), cert. denied, 513 U.S. 1002 (1994); United States v. Vario, 943 F.2d 236 (2d Cir. 1991) (four-year total delay, seven months between when law enforcement realized relevance of tapes to instant case and when the order was obtained), cert. denied, 502 U.S. 1036 (1992); United States v. Van Horn, 789 F.2d 1492 (11th Cir.) (the government's request under section 2517(5) for testimonial use of state wiretap evidence in a federal drug prosecution was timely, although it was made 22 months after federal agents learned of the state wiretap and five months after they learned of the contents of the state wiretap), cert. denied, 479 U.S. 854 (1986); United States v. Arnold, 773 F.2d 823 (7th Cir. 1985) (thirty-one-month delay in seeking order); United States v. Southard, 700 F.2d 1 (1st Cir. 1983) (nineteen-month delay between recording of conversations and application for their use).

The purpose of section 2517(5) is to ensure that the interception of the other offenses was truly incidental to the interception of offenses for which the government had court-authorization. As mentioned previously, with regard to interceptions involving wire and oral communications, the government may only use electronic surveillance to investigate certain crimes and only those crimes; the government cannot allege that it will intercept communications about predicate offenses (those listed under section 2516(1)) and in actuality intercept communications about offenses which are not predicates

under Title III or Title III predicates for which they did not have probable cause. See United States v. London, 66 F.3d 1227 (1st Cir. 1995) ("the interception is unlawful only when it is motivated by an illicit purpose - e.g., 'subterfuge' interceptions where the government applies to intercept conversations relating to offenses specified in 18 U.S.C. § 2516(1) while intending to intercept conversations relating to offenses for which interceptions are unauthorized or which it has no probable cause to obtain an interception order"), cert. denied, 116 S. Ct. 1542 (1996); United States v. Homick, 964 F.2d 899 (9th Cir. 1992); United States v. Ardito, 782 F.2d 358 (2d Cir.), cert. denied, 475 U.S. 1141 (1986); United States v. Van Horn, 789 F.2d 1492 (11th Cir.), cert. denied, 479 U.S. 854 (1986).

"Other" offenses under section 2517(5) may include offenses, federal as well as state, not listed in 18 U.S.C. § 2516, as well as additional predicate offenses not set out in the court order, as long as there is no indication of bad faith or subterfuge on the part of the government. See In re Grand Jury Subpoena Served on Doe, 889 F.2d 384 (2d Cir. 1989) (tax offenses); United States v. Shnayderman, 1993 WL 524782 (E.D. Pa. Dec. 17, 1993) (unreported) (tax offenses).

XII. DISCOVERY

1. 18 U.S.C. § 2518(9), 2518(10)(a)

Section 2518(9) requires the government to furnish a defendant with a copy of the court order and accompanying application under which the interception was authorized or approved, ten days before the contents of any wire, oral, or electronic communication is received in evidence in any trial, hearing, or other proceeding in a federal or state court, unless the court waives the ten-day period upon a showing by the government that compliance is not possible and that the defendant will not be prejudiced. See In re Grand Jury Proceedings, 841 F.2d 1048, 1053 n.9 (11th Cir. 1988) (construing "applications" and "orders" to include related documentation and intercepted conversations).

While section 2518(9) requires the government to disclose wiretap applications and orders to a defendant, the "good cause" requirement of section 2518(8)(b) and the "interest of justice" standard in section 2518(10)(a) make it clear that the defendant is entitled only to that information that is relevant to his defense and is not protected from disclosure by some other constitutional right or privilege. See United States v. Orena, 883 F. Supp. 849 (E.D.N.Y. 1995) ("[t]here is no statutory requirement that all recordings made pursuant to the court order be produced. To the contrary, section 2518(10)(a) specifically provides that it rests within the discretion of the trial court to decide whether intercepted communications should be furnished

to a defendant"); United States v. Yoshimura, 831 F. Supp. 799 (D. Hawaii 1993); Application of U.S. for an Order Authorizing Interception of Wire and Oral Communications, 495 F. Supp. 282 (E.D. La. 1980); United States v. Ferle, 563 F. Supp. 252 (D.R.I. 1983).

2. The Federal Rules

The discovery of electronic surveillance evidence must be made in accord not only with the wiretap statutes, but also with the Federal Rules of Criminal Procedure. For examples, see United States v. Howell, 514 F.2d 710 (5th Cir. 1975), cert. denied, 429 U.S. 838 (1976); United States v. Feola, 651 F. Supp. 1068 (S.D.N.Y. 1987), aff'd, 875 F.2d 857 (1989).

While electronic surveillance evidence and its related documentation are discoverable, work product exposing the government's theory is not. Feola, supra; United States v. Payden, 613 F. Supp. 800 (S.D.N.Y. 1985) (the court denied requests for analysis performed on toll records and other conclusions of investigative officers; these were internal government documents made in connection with the investigation of the case). See also United States v. Nakashian, 635 F. Supp. 761 (S.D.N.Y. 1986) (same), cert. denied, 484 U.S. 963 (1987).

XIII. PEN REGISTERS/TRAPS AND TRACES

ECPA codified Department policy by requiring a court order to install and use a pen register or trap and trace device (18 U.S.C. §§ 3121-3127 (1996)). See United States v. Fregoso, 60 F.3d 1314 (8th Cir. 1995) (caller identification service is a "trap and trace device" as that term is defined in 18 U.S.C. § 3127(4)). The application may be made by an attorney for the government or a state law enforcement or investigative officer, and must certify that the information likely to be obtained is relevant to an ongoing criminal investigation. Unlike Title III pleadings, a pen register application need not establish probable cause and does not require prior Department approval. The order, which is valid for sixty days (and may be extended for additional sixty-day periods), must identify the subscriber of the telephone that is the subject of the order; identify the person, if known, who is the subject of the criminal investigation; identify the number and, if known, the location of the telephone or the geographical limits of a trap and trace (generally stated as being within the territorial jurisdiction of the United States); name the offense(s) to which the information to be obtained from the pen register or trap and trace will relate; and direct the service provider to provide the necessary information and technical assistance to facilitate the court order. The order should also direct that the application and order be sealed, and that no disclosure of the existence of the pen register or trap and trace be made to the subscriber or other persons until directed by the court. See generally Fregoso, supra ("The

judicial role in approving use of trap and trace devices is ministerial in nature"); In re Application of United States for Order Authorizing Installation and Use of Pen Register and Trap and Trace Device, 846 F. Supp. 1555 (M.D. Fla. 1994) (the court must issue a pen register order on mere statutory certification by the government). When seeking a pen register/trap and trace order, the government may obtain the order in the jurisdiction where the telephone is located or in the jurisdiction where the pen register/trap and trace device is monitored. See United States v. Rodriguez, 968 F.2d 130 (2d Cir.), cert. denied, 506 U.S. 847 (1992).

Effective October 25, 1994, section 3121 was amended to include the following new section:

(c) Limitation.--A government agency authorized to install and use a pen register under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing.

This new section was intended to eliminate, when technology permits, pen register recordings of dialed numbers beyond those needed to connect two facilities, such as digital pager messages (codes and return numbers); the latter are substantive electronic communications, the interception of which is properly the subject of a Title III application and interception order under section 2516(3).

Notwithstanding the addition of the limiting language of section 3121(c), the liberal definition of "pen register" in section 3127(3) ("a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached") remains unchanged. Taken literally, this definition does not limit a pen register's recordings to numbers dialed to connect to other telephones or pagers. It should be noted, however, that the statutory definition of "trap and trace device" in section 3127(4) ("a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted") limits precisely the numbers that can be captured to those which identify the originating number.

The legislative history of the original ECPA pen register provision contains the following language:

[T]he term "pen register" means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted for purposes of routing telephone calls, with respect to wire communications, on the telephone line to which such device is attached. Pen registers do not record

the contents of a communication. They record only the telephone numbers dialed.

S. Rep. No. 541, 99th Cong., 2d Sess. 49 (1986)

Pen registers are devices that record the telephone numbers to which calls have been placed from a particular telephone. These capture no part of an actual telephone conversation, but merely the electronic switching signals that connect two telephones. [From the "Glossary"]

S. Rep. No. 541, 99th Cong., 2d Sess. 10 (1986)

The legislative history of the 1994 amendment asserts that the new amendment prohibits the use of pen register and trap and trace orders to obtain tracking or location information, noting that it:

further protects privacy by...restricting the ability of law enforcement to use pen register devices for tracking purposes or for obtaining transactional information.

* * *
expressly provides that the authority under pen register and trap and trace orders cannot be used to obtain tracking or location information, other than that which can be determined from the phone number. Currently, in some cellular systems, transactional data that could be obtained by a pen register may include location information. Further, the bill requires law enforcement to use reasonably available technology to minimize information obtained through pen registers.

* * *
requires government agencies installing and using pen register devices to use, when reasonably available, technology that restricts the information captured by such device to the dialing or signaling information necessary to direct or process a call, excluding any further communication conducted through the use of dialed digits that would otherwise be captured.

H. Rep. No. 827, 103rd Cong., 2d Sess. 10, 17, 32 (1994).

At the present time, the technology is not available that can discern and record or decode those numbers dialed solely for the purpose of connecting two telephones.

XIV. CELL SITE SIMULATORS/DIGITAL ANALYZERS

1. Definition

A cell site simulator or a digital analyzer can electronically force a cellular telephone to register its mobile identification number ("MIN," i.e., telephone number) and electronic serial number ("ESN," i.e., the number assigned by the manufacturer of the cellular telephone and programmed into the telephone) when the cellular telephone is turned on but is not

being used. Cell site data (the MIN, the ESN, and the channel and cell site codes identifying the cell location and geographical sub-sector from which the telephone is transmitting) are being transmitted continuously as a necessary aspect of cellular telephone call direction and processing. The necessary signaling data (ESN/MIN, channel/cell site codes) are not dialed or otherwise controlled by the cellular telephone user. Rather, the transmission of the cellular telephone's ESN/MIN to the nearest cell site occurs automatically when the cellular telephone is turned on. This automatic registration with the nearest cell site is the means by which the cellular service provider connects with and identifies the account, knows where to send calls, and reports constantly to the customer's telephone a read out regarding the signal power, status and mode.

If the cellular telephone is used to make or receive a call, the read out on the screen of the digital analyzer/cell site simulator would include the cellular telephone number (MIN), the call's incoming or outgoing status, the telephone number dialed, the cellular telephone's ESN, the date, time, and duration of the call, and the cell site number/sector (location of the cellular telephone when the call was connected). Because digital analyzers/cell site simulators are capable of intercepting wire communications, they must be programmed to capture only the cell site activity of the cellular telephone, unless a Title III interception order has been obtained.

2. Applicability of 18 U.S.C. §§ 3121-3127

As discussed above, section 3121(c) requires law enforcement to use technology reasonably available to limit a pen register's capture of data to dialing/signaling information. As worded, this section would appear to permit a pen register, and likewise a cell site simulator and digital analyzer, to record or decode cell site information that is transmitted automatically and continuously over radio waves to process cellular communications. Accordingly, there appears to be no bar within 18 U.S.C. §§ 3121-3127 to the capture of this data, using a cell site simulator or digital analyzer. In In The Matter Of The Application Of The United States Of America For An Order Authorizing The Use Of A Cellular Telephone Digital Analyzer, 885 F. Supp. 197 (C.D. Cal. 1995), the court held that no court order was required to use a digital analyzer to capture a cellular telephone's ESN and MIN.

The court in Digital Analyzer went further and reasoned that because a digital analyzer does not attach to the cellular telephone, this device does not fall within the statutory definition of a pen register and, therefore, no court order is required to use a digital analyzer to record the numbers dialed from a cellular telephone. The court did, however, outline how the pen register application and order should be drafted if the government chose to file those pleadings.

Despite the opinion in Digital Analyzer, it is the Department's recommendation that to the extent cell site simulators, digital analyzers, and related technology are used as pen registers or trap and trace devices, they should only be used pursuant to court orders issued under 18 U.S.C. §§ 3121-3127.

3. Non-Applicability of Title III

Title III does not apply to the use of digital analyzers and cell site simulators when they are used to capture signaling and call processing information because, when so used, these devices do not intercept the contents of any wire, oral, or electronic communication as the term "contents" is defined by Title III. Currently, section 2510(8) states, "'contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." ESNs/MINs and other automatic (not dialed by the user) signaling and registration information technologically necessary to the service provider's processing of cellular calls is not the type of transmission Congress included within section 2510(8)'s definition of "contents," when Title III was amended by ECPA in 1986. Congress stated that ECPA:

...amends current section 2510(8) of title 18 to exclude from the definition of the term "contents," the identity of the parties or the existence of the communication. It thus distinguishes between the substance, purport or meaning of the communication and the existence of the communication or transactional records about it.

S. Rep. No. 541, 99th Cong., 2d Sess. 13 (1986).

Because cell site information (ESN/MIN, channel/sector, cell site code) concerns only the identity of the parties and the existence of the communication, but not the substance, purport, or meaning of the communication, it can be characterized properly as "transactional records about" wire communications on a cellular system.

In addition, as Title III (18 U.S.C. § 2511(2)(h)(i)) specifically exempts the use of pen registers and trap and trace devices from the constraints of Chapter 119 of Title 18, it would be reasonable to argue that a similar exclusion, in the absence of clarifying statutory language, should apply to digital analyzers/cell site simulators. As discussed previously, these devices capture signaling information (ESN/MIN, channel/sector, cell site code) that is being constantly and automatically transmitted between cellular antennae sites and cellular telephone units without the users' knowledge, but as a necessary aspect of the technology that enables the service provider to process the users' cellular communications.

4. Non-Applicability of 18 U.S.C. § 2703

If, rather than a contemporaneous electronic communication covered by Title III, cell site information is treated as a subscriber record or other information, it could be argued that section 2703 might apply. It should be noted, however, that section 2703 controls disclosures by service providers to governmental entities and does not prohibit the government from obtaining such information on its own, without involving the service provider. Additionally, because cell site simulators and digital analyzers do not obtain access to communications in electronic storage in a facility through which an electronic communication service is provided, section 2703 is likewise not implicated.

5. Conclusion

To the extent these devices are used to capture cellular signaling and processing information not dialed or otherwise intentionally transmitted by the user, and concern only the identification of the telephone numbers for the parties and the existence of a communication, the acquisition of this cell site information does not require an order under Title III, 18 U.S.C. § 2703, or 18 U.S.C. §§ 3121-3127.

Caution should be exercised regarding the devices' capabilities regarding the contents of wire or electronic communications. Careful analysis of the technical treatment of such communications by the monitoring device is necessary to avoid possible violations of Title III through the capture, acquisition, diversion, temporary storage, or other manipulation of transmissions occurring over the separate voice channel of the cellular system, even though they are not heard by the human ear.

XV. MOBILE TRACKING DEVICES

Tracking devices ("bumper beepers") are not regulated by Title III, and their use is governed by existing case law. The seminal cases in this area are United States v. Knotts, 460 U.S. 276 (1983) (Fourth Amendment not implicated) and United States v. Karo, 468 U.S. 705 (1984) (warrantless monitoring in an area invoking a reasonable expectation of privacy may violate Fourth Amendment), which set forth the Fourth Amendment standards governing the use of beepers. Basically, a search warrant is needed only when the object to which the beeper is attached enters an area that carries a legitimate expectation of privacy, such as the inside of a vehicle or a private residence. Since it often cannot be determined in advance whether a package containing a beeper will be taken inside a place where a person has a valid expectation of privacy, a search warrant should be obtained. But see United States v. Jones, 31 F.3d 1304 (4th Cir. 1994) (Postal Inspectors' use of an electronic tracking device to monitor movement of a stolen mail pouch that defendant placed in

his van did not constitute a search within the ambit of the Fourth Amendment).

ECPA did, however, change the existing jurisdictional requirement relating to tracking devices. 18 U.S.C. § 3117 provides that a court order issued for such a device is valid anywhere within the United States. This obviates the need to obtain a new order whenever the object containing the device crosses state or district lines.

XVI. VIDEO SURVEILLANCE

Video surveillance, or the use of closed circuit television (CCTV), is not regulated by Title III, but is frequently part of an application for electronic surveillance. When there is a reasonable expectation of privacy in the place to be videotaped, prior approval from an appropriate DOJ official and a court order are required before such video surveillance may be used in an investigation. Briefly, a court order and prior Department approval are required unless the surveillance is used to record events in public places or places where the public has unrestricted access, and where the camera equipment can be installed in places to which investigators have lawful access. See generally Thompson v. Johnson County Community College, 930 F. Supp. 501 (D. Kan. 1996) (college's warrantless use of CCTV to monitor locker area of storage room for thefts and weapons was constitutional).

If a court order is required, the pleadings are to be based on Rule 41(b) of the Federal Rules of Criminal Procedure and the All Writs Act (28 U.S.C. § 1651). The courts of appeals in six circuits, while recognizing that video surveillance does not fall within the letter of Title III, require that applications to use video surveillance of suspected criminal activities meet most of the higher constitutional standards required under Title III. Therefore, the application and order should be based on an affidavit that establishes probable cause to believe that evidence of a federal crime will be obtained by the surveillance, and should also include: (1) a statement indicating that normal investigative procedures have been tried and failed or reasonably appear to be unlikely to succeed if tried or are too dangerous; (2) a particularized description of the premises to be surveilled; (3) the names of the persons to be surveilled, if known; (4) a statement of the steps to be taken to ensure that the surveillance will be minimized to effectuate only the purposes for which the order is issued; and (5) a statement of the duration of the order, which shall not be longer than is necessary to achieve the objective of the authorization, or in any event no longer than thirty days (a ten-grace period is not permitted; the time period begins to run from the date of the order). United States v. Falls, 34 F.3d 674 (8th Cir. 1994); United States v. Koyomejian, 970 F.2d 536 (9th Cir.) (en banc), cert. denied, 506 U.S. 1005 (1992); United States v. Mesa-Rincon,

911 F.2d 1433 (10th Cir. 1990); United States v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987); United States v. Biasucci, 786 F.2d 504 (2d Cir. 1986), cert. denied, 479 U.S. 827 (1986); United States v. Torres, 751 F.2d 875 (7th Cir. 1984), cert. denied sub nom. Rodriguez v. United States, 470 U.S. 1087 (1985).

When the government wants to intercept oral communications as well as video images within the same target premises, the same affidavit may be used to establish probable cause for the use of the microphone and the camera. Separate applications and orders, however, should be filed for each type of interception because each is governed by a different standard, and the pleadings should reflect this difference. As noted above, Title III regulates the interception of oral communications (as well as wire and electronic), and Rule 41 and the body of case law cited above establish the parameters in which video surveillance may be used for law enforcement purposes.

Consensual video surveillance does not violate the Fourth Amendment and, therefore, no court order is required. United States v. Cox, 836 F. Supp. 1189 (D. Md. 1993) (cooperating defendant consented to video monitoring of motel room, was in the room at all times, and the surveillance did not pick up any words or actions that were outside the consenting party's hearing and sight).

XVII. CONSENSUAL MONITORING

1. Consensual Monitoring by Law Enforcement

Neither Title III (18 U.S.C. § 2511(2)(c)) nor the Fourth Amendment prohibits a law enforcement officer or a person acting under color of law⁴ from intercepting a wire, oral, or electronic communication without a court order when one of the parties to the communication has consented to the interception. See United States v. Caceres, 440 U.S. 741 (1979); United States v. White, 401 U.S. 745 (1971); United States v. McKneely, 69 F.3d 1067 (10th Cir. 1995) (cooperating defendant voluntarily consented to audio and video surveillance of her hotel room); United States v. Laetividal-Gonzalez, 939 F.2d 1455 (11th Cir. 1991) (undercover agent could consent to recording of conversation with defendant), cert. denied, 503 U.S. 912 (1992); United States v. Miller, 720

⁴ Courts have held repeatedly that informants who tape-record private conversations at the direction of government investigators are "acting under color of law" within the meaning of section 2511(2)(c). See Obron Atlantic Corporation v. Barr, 990 F.2d 861 (6th Cir. 1993) (continuous but irregular contact with DOJ attorneys following their request for assistance and their instructions on how to conduct the calls); United States v. Haimowitz, 725 F.2d 1561 (11th Cir.) (FBI "supervised" the taping conducted by the informant), cert. denied, 469 U.S. 1072 (1984).

F.2d 227 (1st Cir. 1983) (defendant knew cooperating witness was listening in on three-way conference call), cert. denied, 464 U.S. 1073 (1984); United States v. Shields, 675 F.2d 1152 (11th Cir.) (government properly intercepted conversations by way of a tape recorder installed by cooperating detective at the request of the defendant), cert. denied, 459 U.S. 858 (1982); United States v. Cox, 836 F. Supp. 1189 (D. Md. 1993) (cooperating defendant consented to audio and video surveillance of his motel room).

Compare these cases with United States v. Kim, 803 F. Supp. 352 (D. Hawaii 1992) (holding that the agent was not a party to the communication) and United States v. Shabazz, 883 F. Supp. 422 (D. Minn. 1995) (citing United States v. Padilla, 520 F.2d 526 (1st Cir. 1975), the court held that the informant had no right to consent to the placement of recording devices in the subject's hotel room; the court was concerned that the government was free to surveil at will).

The Department has developed guidelines for the investigative use of consensual electronic surveillance in certain situations. These guidelines, which are set forth in full in the USAM, Chapter 9, Title 7, require that in certain, specified sensitive situations, law enforcement agencies must obtain advance authorization from the Department before employing consensual monitoring. The guidelines cover the investigative use of devices that intercept and record certain consensual, verbal conversations when a body transmitter or recorder, or a fixed location transmitter or recorder, is used during a face-to-face conversation. The guidelines do not apply to consensual monitoring of telephone conversations or radio transmissions. It was left to the law enforcement agencies to develop adequate internal guidelines for the use of those types of consensual monitoring.

2. Consensual Monitoring by Private Parties

Under 18 U.S.C. § 2511(2)(d), an individual may intercept an oral, wire, or electronic communication if that person is a party to the communication or a party to the communication has given consent,⁵ provided the interception was not made for a criminal or tortious purpose.

⁵ Williams v. Poulos, 11 F.3d 271 (1st Cir. 1993) (while the employee was advised of monitoring, it was not clear that he was told about the manner in which the monitoring would be conducted and that he would be subject to monitoring; consent was not implied); Griggs-Ryan v. Smith, 904 F.2d 112 (1st Cir. 1990) (plaintiff was warned several times that all calls would be monitored); Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983) (knowledge of monitoring capability does not result in implied consent).

A person seeking to suppress a consensual tape recording bears the burden of proving by a preponderance of the evidence that the defendant's primary motivation, or a determinative factor in the defendant's motivation, for intercepting the conversation was to commit a criminal, tortious, or other injurious act. See Desnick v. American Broadcasting Companies, Inc., 44 F.3d 1345 (7th Cir. 1995) (broadcaster's use of test patients with concealed cameras to investigate clinic did not violate federal law; there was no evidence that testers were sent to the clinic for the purpose of committing a crime or a tort); United States v. Zarnes, 33 F.3d 1454 (7th Cir. 1994) (ex-wife made tape for the lawful purpose of potentially seeking leniency with the government), cert. denied, 515 U.S. 1126 (1995); United States v. Cassiere, 4 F.3d 1006 (1st Cir. 1993) (tape was made "to prevent future distortions by a participant"); United States v. Underhill, 813 F.2d 105 (6th Cir.) ("the legality of an interception is determined by the purpose for which the interception is made, not by the subject of the communications intercepted"), cert. denied, 484 U.S. 821 (1987).

The fact that the consenting party may have violated state law requiring consent by all parties does not, by itself, establish that the consenting party intercepted the conversations for the purpose of committing any criminal or tortious act in violation of the state law. See Payne v. Norwest Corporation, 911 F. Supp. 1299 (D. Mont. 1995); Roberts v. Americable Intern. Inc., 883 F. Supp. 499 (E.D. Cal. 1995); United States v. DiFelice, 837 F. Supp. 81 (S.D.N.Y. 1993).

XVIII. CUSTODIAL MONITORING

1. Law Enforcement Access to Monitored Prison Calls

In 1987, the Criminal Division established guidelines for the Bureau of Prisons (BOP) on law enforcement access to electronically monitored and intercepted inmate telephone calls. In short, the Division requires law enforcement to obtain a court order or a subpoena to obtain inmate telephone calls in connection with a criminal investigation. While this requirement seemingly exceeds the legal requirements regarding law enforcement access to monitored prison calls, it ensures BOP's future ability to monitor inmate calls by diminishing the risk that access to them will not exceed the bounds of propriety. By not testing the courts' tolerance of inmate monitoring, the Division is protecting the monitoring program. In addition, the requirement of a court order or subpoena protects the privacy interests of members of the public who have a privacy interest in their phone calls and the arguable privacy interest that inmates may have in personal calls which do not implicate prison security. See United States v. Green, 842 F. Supp. 68 (W.D.N.Y. 1994) (recordings focused on a particular inmate and made to gather evidence for a criminal investigation was not monitoring in the ordinary course of business; tapes nevertheless admissible

under theory of implied consent), cert. denied, 117 S. Ct. 373 (1996); Langton v. Hogan, 71 F.3d 930 (1st Cir. 1995) (debatable whether implied consent can be given freely and voluntarily in a prison setting). See also an opinion by the Office of Legal Counsel (OLC), dated January 14, 1997, in which OLC cautioned that the monitoring of a particular inmate's telephone calls for purposes unrelated to prison security or administration "may jeopardize the application of the ordinary course of duties exception" to Title III. OLC stated further that such a result would be "fatal in jurisdictions that reject the implied consent theory of monitoring."

Briefly, the Division's policy is as follows: in the event that a telephone conversation, monitored routinely by prison officials for the purpose of prison security, is found to contain information relating to the violation of federal or state law, prison officials may disclose that information to the proper law enforcement authorities for further investigation and/or prosecution. Law enforcement authorities outside the Bureau of Prisons should not be allowed random access to inmate monitored telephone calls, past, present or future.

In those cases when outside law enforcement agencies request Bureau of Prisons officials to disclose transcripts of the general telephone conversations of inmates that have been monitored in the past in connection with a criminal investigation being conducted of activities outside the confines of the prison, and the request concerns specified individuals, the information requested should be disclosed only pursuant to a grand jury subpoena or other process.

In those cases when outside law enforcement agencies ask Bureau of Prisons officials to monitor and disclose the future telephone conversations of specified inmates in connection with a criminal investigation being conducted of activities outside the confines of the prison, not affecting prison security or administration, this monitoring should be conducted only when an interception order has been procured under the authority of Title III.

2. Case Law on Custodial Monitoring

The courts have upheld warrantless monitoring of a prisoner's telephone conversations under one of two theories, consent (18 U.S.C. § 2511(2)(c))⁶ or the law enforcement

⁶ 18 U.S.C. § 2511(2)(c) ("It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties has given prior consent to such interception."). See also United States v. Workman, 80 F.3d 688 (2d Cir. 1996); United States v. Van Poyck,

exception (18 U.S.C. § 2510(5)(a)).⁷ Occasionally, the courts have held that neither exception applies. See Campiti v. Walonis, 611 F.2d 387 (1st Cir. 1979) (holding police officer civilly liable after finding that no exception applied to situation when police officer used an extension telephone to intercept calls between inmates); In re State Police Litigation, 888 F. Supp. 1235 (D. Conn. 1995) (improper to record telephone calls to and from state police barracks when neither caller consented to the recording).

In most custodial settings, an inmate will not be able to argue successfully that a reasonable expectation of privacy exists in face-to-face conversations. See Siripongs v. Calderon, 35 F.3d 1308 (9th Cir. 1994) (surreptitious tape recording of defendant's side of a telephone conversation did not violate Title III); United States v. Clark, 22 F.3d 799 (8th Cir. 1994) (no reasonable expectation of privacy in a marked police car); Angel v. Williams, 12 F.3d 786 (8th Cir. 1993) (police officers did not have a reasonable expectation of privacy that their conversations with an inmate in a public jail would not be intercepted); United States v. McKinnon, 985 F.2d 525 (11th Cir. 1993) (marked police car); United States v. Veilleux, 846 F. Supp. 149 (D.N.H. 1994) (prisoner had no reasonable expectation of privacy in his holding cell and one-sided telephone conversations, which were overheard by guarding officer who was within earshot).

77 F.3d 285 (9th Cir. 1996); United States v. Horr, 963 F.2d 1124 (8th Cir. 1992).

⁷ 18 U.S.C. § 2510(5)(a) ("electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than (a) any telephone or telegraph instrument, equipment or facility, or any component thereof... (ii) being used ... by an investigative or law enforcement officer in the ordinary course of his duties"). See also United States v. Van Poyck, 77 F.3d 285 (9th Cir. 1996); United States v. Sababu, 891 F.2d 1308 (7th Cir. 1989); United States v. Paul, 614 F.2d 115 (6th Cir. 1980); United States v. Noriega, 764 F. Supp. 1480 (S.D. Fla. 1991).

Application for Wire and/or Oral Interceptions

(FORM 1)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA FOR
AN ORDER AUTHORIZING THE INTERCEPTION
OF (WIRE) (ORAL) COMMUNICATIONS

APPLICATION FOR INTERCEPTION OF (WIRE) (ORAL) COMMUNICATIONS

_____, Assistant United States Attorney,
District of _____, being duly sworn,
states:

1. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, that is, an attorney authorized by law to prosecute or participate in the prosecution of offenses enumerated in Section 2516 of Title 18, United States Code.

2. This application is for an order pursuant to Section 2518 of Title 18, United States Code, authorizing the interception of (wire) (oral) communications until the attainment of the authorized objectives or, in any event, at the end of thirty (30) days from the earlier of the day on which the investigative or law enforcement officers first begin to conduct an interception under the Court's order or ten (10) days after the order is entered, of (list those persons who will be intercepted over the telephone or within the premises, "interceptees") and others as yet unknown (if wire: "to and from the telephone(s) bearing the number(s) _____, subscribed to by _____ and located at/billed to _____") (if oral: "occurring inside the premises located at _____" or

"occurring in and around a (describe the make, color and year of the vehicle) bearing the license plate number _____ and the vehicle identification number _____") concerning offenses enumerated in Section 2516 of Title 18, United States Code, that is, offenses involving violations of (list section(s) of the U.S. Code and describe briefly the applicable offense(s)) that are being committed by (list the interceptees and those persons who are also part of the conspiracy but may not necessarily be intercepted over the target facility or within the target

premises/vehicle, collectively they are referred to as "violators,") and others as yet unknown.

3. Pursuant to Section 2516 of Title 18, United States Code, the Attorney General of the United States has specially designated the Assistant Attorney General, any Acting Assistant Attorney General, any Deputy Assistant Attorney General or any acting Deputy Assistant Attorney General of the Criminal Division (or, in the case of a roving interception, the Assistant Attorney General or Acting Assistant Attorney General in the Criminal Division) to exercise the power conferred on the Attorney General by Section 2516 of Title 18, United States Code, to authorize this Application. Under the power designated to him by special designation of the Attorney General pursuant to Order Number - _____ (currently 95-1950) of _____ (currently February 13, 1995), an appropriate official of the Criminal Division has authorized this Application. Attached to this Application are copies of the Attorney General's order of special designation and the Memorandum of Authorization approving this Application.

4. I have discussed all of the circumstances of the above offenses with Special Agent _____ of the (name the investigative agency), who has directed and conducted this investigation and have examined the Affidavit of Special Agent _____, which is attached to this Application and is incorporated herein by reference. Based upon that Affidavit, your applicant states upon information and belief that:

a. there is probable cause to believe that (list the violators) and others as yet unknown have committed, are committing, and will continue to commit violations of (list the offenses - must be enumerated in Section 2516 of Title 18, United States Code);

b. there is probable cause to believe that particular (wire) (oral) communications of (name the interceptee(s)) concerning the above-described offenses will be obtained through the interception of (wire) (oral) communications. In particular, these (wire) (oral) communications will concern the (characterize the types of criminal communications expected to be intercepted). In addition, the communications are expected to constitute admissible evidence of the commission of the above-stated offenses;

c. normal investigative procedures have been tried and failed, reasonably appear to be unlikely to succeed if tried, or are too dangerous to employ, as is described in further detail in the attached Affidavit;

d. there is probable cause to believe that (identify fully the telephone(s) from which, or the premises where, the wire or oral communications are to be intercepted)

is/are being used and will continue to be used in connection with the commission of the above-described offenses.

(If a roving interception, add the following language:

"The attached affidavit contains information demonstrating, within the meaning of Title 18, United States Code, Section 2518 (11)(a) and/or (b), that (if oral: "specification of the place(s) where communications of (name the interceptees) are to be intercepted is not practical") (if wire: "that (name the person(s)) use(s) various and changing facilities for the purpose of circumventing and thwarting interception.")).

5. The attached Affidavit contains a full and complete statement of facts concerning all previous applications which are known to have been made to any judge of competent jurisdiction for approval of the interception of the oral, wire or electronic communications of any of the same individuals, facilities, or premises specified in this Application. (If there has been no previous electronic surveillance, state: "The applicant is aware of no previous applications made to any judge for authorization to intercept the oral, wire or electronic communications of any of the persons or involving the (facilities) (premises) specified in this application.")

WHEREFORE, your applicant believes that there is probable cause to believe that (name the violators) and others as yet unknown are engaged in the commission of offenses involving (cite to the offenses), that (name the interceptees) and others yet unknown are using (the telephone bearing the number _____, subscribed to by _____ and located at/billed to _____) and/or (the premises or vehicle described as _____) in connection with the commission of the above-described offenses; and that (wire) (oral) communications of (name the interceptees) and others yet unknown will be intercepted (over the above-described telephone facility) and/or (within the above-described premises or the above-described vehicle).

Based on the allegations set forth in this application and on the affidavit of Special Agent _____, attached, the applicant requests this court to issue an order pursuant to the power conferred upon it by Section 2518 of Title 18, United States Code, authorizing the (investigative agency) to intercept (wire communications to and from the above-described facility(ies)) and/or (oral communications from the above-described premises) until such communications are intercepted that reveal the manner in which the named violators and others unknown participate in the specified offenses and reveal the identities of (his)(their) coconspirators, place(s) of operation, and nature of the conspiracy, or for a period of (not to exceed 30 days) measured from the day on which the investigative or law enforcement officers first begin to conduct

the interception or ten days from the date of this order, whichever occurs first.

(If interception of oral communications is requested, add:

IT IS REQUESTED FURTHER that this Court issue an order pursuant to Section 2518 of Title 18, United States Code, authorizing Special Agents of the (name investigative agency) to make all necessary surreptitious and/or forcible entries to effectuate the purposes of this Court's Order, including entries to install, maintain, and remove electronic listening devices from (describe the premises/vehicle). The applicant shall notify the Court of any surreptitious entry.)

(If interception of wire communications is requested, add:

IT IS REQUESTED FURTHER that the authorization given be intended to apply not only to the target telephone number(s) listed above, but to any changed telephone number subsequently assigned to the same cable, pair, and binding posts utilized by the target telephone(s) within the thirty (30) day period. (If the telephone is a cellular telephone, the language should state: "the authorization given be intended to apply not only to the target telephone number(s) listed above, but to any changed telephone number or any other telephone number subsequently assigned to or used by the instrument bearing the same electronic serial number as the target cellular phone within the thirty (30) day period.") It is also requested that the authorization be intended to apply to background conversations intercepted in the vicinity of the target telephone(s) while the telephone(s) is off the hook or otherwise in use.)

(If multi-jurisdictional authorization for a portable/mobile facility is requested, add:

IT IS REQUESTED FURTHER that in the event that the target facility/vehicle is transferred outside the territorial jurisdiction of this Court, interceptions may take place in any other jurisdiction within the United States.)

(If a roving interception is requested, add:

IT IS REQUESTED FURTHER that this Court issue an order authorizing the roving interception of the (wire) (oral) communications of (name the target(s)) (if wire: "from various and changing telephone facilities), (if oral: "from various locations in (name the jurisdiction) that it are not practical to specify) as provided in Title 18, United States Code, Section 2518(11)(a) or (b) and as specifically authorized by the (Acting) Assistant Attorney General of the Criminal Division, for a thirty (30) day period.)

(If wire communication, add:

IT IS REQUESTED FURTHER that this Court issue an order pursuant to Section 2518(4) of Title 18, United States Code, directing the (name the communications service provider(s)), an electronic communications service provider as defined in Section 2510(15) of Title 18, United States Code, to furnish and continue to furnish the (investigative agency) with all information, facilities and technical assistance necessary to accomplish the interceptions unobtrusively and with a minimum of interference with the services that such providers are according the persons whose communications are to be intercepted, and to ensure an effective and secure installation of electronic devices capable of intercepting wire communications over the above-described telephone. The service provider shall be compensated by the Applicant for reasonable expenses incurred in providing such facilities or assistance.)

IT IS REQUESTED FURTHER, to avoid prejudice to this criminal investigation, that the Court order the providers of electronic communication service and their agents and employees not to disclose or cause a disclosure of this Court's Order or the request for information, facilities, and assistance by the (investigative agency) or the existence of the investigation to any person other than those of their agents and employees who require this information to accomplish the services requested. In particular, said providers and their agents and employees should be ordered not to make such disclosure to a lessee, telephone subscriber, or any interceptee or participant in the intercepted communications.

IT IS REQUESTED FURTHER that this Court direct that its Order be executed as soon as practicable after it is signed and that all monitoring of (wire) (oral) communications shall be conducted in such a way as to minimize the interception and disclosure of the communications intercepted to those communications relevant to the pending investigation, in accordance with the minimization requirements of Chapter 119 of Title 18, United States Code. The interception of (wire) (oral) communications authorized by this Court's Order must terminate upon attainment of the authorized objectives or, in any event, at the end of thirty (30) days measured from the day on which investigative or law enforcement officers first begin to conduct an interception or ten (10) days after the Order is entered.

Monitoring of conversations must immediately terminate when it is determined that the conversation is unrelated to communications subject to interception under Chapter 119 of Title 18, United States Code. Interception must be suspended immediately when it is determined through voice identification, physical surveillance, or otherwise, that none of the named interceptees or any of their confederates, when identified, are participants in the conversation unless it is determined during

the portion of the conversation already overheard that the conversation is criminal in nature.

IT IS REQUESTED FURTHER that the Court order that either (Applicant/AUSA) or any other AUSA familiar with the facts of the case provide the Court with a report on or about the (tenth), (twentieth) and (thirtieth) days following the date of this Order showing what progress has been made toward achievement of the authorized objectives and the need for continued interception. If any of the aforementioned reports should become due on a weekend or holiday, it is requested further that such report become due on the next business day thereafter.

IT IS REQUESTED FURTHER that the Court order that its Orders, this application and the accompanying affidavit and proposed Order(s), and all interim reports filed with the Court with regard to this matter be sealed until further order of this Court, except that copies of the Order(s), in full or redacted form, may be served on the (name the investigative agency/agencies) and the service provider(s) as necessary to effectuate the Court's Order as set forth in the proposed order(s) accompanying this application.

DATED this _____ day of _____, 199__.
(Name and title of the applicant)

(NAME)
Assistant United States Attorney

SUBSCRIBED and SWORN to before me
this _____ day of _____, 199__.

UNITED STATES DISTRICT COURT JUDGE
(District)

Affidavit for Oral and/or Wire Interception

(FORM 2)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA FOR)
AN ORDER AUTHORIZING THE INTERCEPTION)
OF (WIRE) (ORAL) COMMUNICATIONS)

AFFIDAVIT IN SUPPORT OF APPLICATION

INTRODUCTION

_____, being duly sworn, deposes and states as follows:

1. I am a Special Agent with the _____, United States Department of Justice. I have been so employed by the (name the agency) for the past _____ () years. I have participated in investigations involving (organized crime/drug trafficking/money laundering, etc.) activities for the past _____ () years. (Describe present assignment.)

2. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code.

3. This affidavit is submitted in support of an application for an order authorizing the interception of (wire) (oral) communications occurring (describe the facility or premises to which the application and affidavit are directed).

4. I have participated in the investigation of the above offenses. As a result of my personal participation in this investigation, through interviews with and analysis of reports submitted by other (Special Agents of the _____ and/or other state/local law enforcement personnel), I am familiar with all aspects of this investigation. On the basis of this familiarity, and on the basis of other information which I have reviewed and determined to be reliable, I allege the facts to show that:

a. there is probable cause to believe that (name the violators) are committing, and will continue to commit violations of (list the offenses - must be ones enumerated in Section 2516 of Title 18, United States Code);

b. there is probable cause to believe that particular (wire)(oral) communications of (name the interceptees) concerning the above offenses will be obtained through the interception of such communications (if wire: "to and from the telephone(s) bearing the number(s) _____, subscribed to by _____ and located at/billed to _____"; if oral: "occurring within premises located at _____" or "occurring in and around a (indicate the make, model and year of the vehicle) bearing the license plate _____ and vehicle identification number _____"); if a roving wire interception: "over various and changing facilities within (identify the jurisdiction) used by (name the particular interceptee(s) - do not include the language "and others yet unknown"); if a roving oral interception: "within presently unknown premises used by (name the particular interceptee(s) - do not include the language "and others yet unknown") that it is impractical to specify.").

In particular, these communications are expected to concern the specifics of the above offenses, including (i) the nature, extent and methods of the (describe the illegal activity) business of (name the violators) and others; (ii) the nature, extent and methods of operation of the business of (name the violators) and others; (iii) the identities and roles of accomplices, aiders and abettors, co-conspirators and participants in their illegal activities; (iv) the distribution and transfer of the contraband and money involved in those activities; (v) the existence and location of records; (vi) the location and source of resources used to finance their illegal activities; (vii) the location and disposition of the proceeds from those activities; and (viii) the locations and items used in furtherance of those activities. In addition, these (wire)(oral) communications are expected to constitute admissible evidence of the commission of the above-described offenses.

The statements contained in this affidavit are based in part on information provided by Special Agents of the (name the investigative agency/agencies), on conversations held with detectives and officers from the (identify the local/state police department), on information provided by confidential sources, and on my experience and background as a Special Agent of the _____. Since this affidavit is being submitted for the limited purpose of securing authorization for the interception of (wire)(oral) communications, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish the necessary foundation for an order authorizing the interception of (oral)(wire) communications.

PERSONS EXPECTED TO BE INTERCEPTED

Include a short description of each known violator; if appropriate, explain why certain participants in the offenses are

not expected to be interceptees. If applicable, note which persons are currently facing pending state or federal criminal charges.

FACTS AND CIRCUMSTANCES

Provide an in-depth discussion of the facts in support of the probable cause statements set forth above. If informant information provides a basis for any of the required information, provide adequate qualifying language for each informant. Remember that you must show probable cause 1) that the alleged offenses are being committed; 2) that the named subjects and others unknown are committing them; and 3) that the targeted telephone(s) and/or premises is/are being used to commit these offenses. It is Department of Justice policy that pen register or telephone toll information for the target telephone(s), or physical surveillance of the targeted premises, standing alone, is generally insufficient to establish probable cause. Probable cause to establish criminal use of the facilities or premises requires independent evidence of use in addition to pen register or surveillance information, e.g. informant or undercover information. On rare occasions, criminal use of the target facilities or premises may be established by an extremely high volume of calls to other known or suspected coconspirators that coincides with incidents of illegal activity, or by a regular pattern of telephone or premises use involving known or suspected coconspirators going back for a period of years.

When requesting a roving wire interception, you must establish that the specifically targeted subject(s) uses various and changing facilities for the purpose of avoiding electronic surveillance (see 18 U.S.C. § 2518(11)(b)(ii)). This purpose may be evinced either by informant information (e.g., the subject's past or current statements to that effect) or by the subject's actions over a period of time (e.g., physical surveillance establishing that the subject travels from phone to phone to call other coconspirators). Roving wiretaps will be authorized for public and cellular telephones only, and only when it is clear that the telephones cannot be identified in advance, and the subject's intent to avoid electronic surveillance is manifested clearly.

In roving oral interceptions (see 18 U.S.C. § 2518(11)(a)(ii)), you must establish probable cause that it is not practical to specify the place where the oral communications of the targeted individual(s) are to be intercepted. Once again, a roving oral interception will be authorized only for public facilities, vehicles, hotel rooms, or similar locations, and a pattern of activity demonstrating the impracticability of naming specific premises must be established.

NEED FOR INTERCEPTION

Need for (Wire) (Oral) Interception

Based upon your affiant's training and experience, (as well as the experience of the other (Special Agents of the _____ and/or state/local officers), and based upon all of the facts set forth herein, it is your affiant's belief that the interception of (wire) (oral) communications is the only available technique that has a reasonable likelihood of securing the evidence necessary to prove beyond a reasonable doubt that (name the violators), and others as yet unknown are engaged in the above-described offenses.

Your affiant states that the following investigative procedures, which are usually employed in the investigation of this type of criminal case, have been tried and have failed, reasonably appear to be unlikely to succeed if they are tried, or are too dangerous to employ.

ALTERNATIVE INVESTIGATIVE TECHNIQUES

Physical Surveillance

(The following is an example of language that discusses the use of physical surveillance in general; you should also discuss the effectiveness of this, and the following other investigative techniques, as they are applicable to your particular case.)

Physical surveillance has been attempted on numerous occasions during this investigation. Although it has proven valuable in identifying some activities and associates of (list the violators), physical surveillance, if not used in conjunction with other techniques, including electronic surveillance, is of limited value. Physical surveillance, even if highly successful, has not succeeded in gathering sufficient evidence of the criminal activity under investigation. Physical surveillance of the alleged conspirators will not (has not) established conclusively the elements of the violations and has not and most likely will not establish conclusively the identities of various conspirators. In addition, (continued) surveillance is not expected to enlarge upon information now available; rather, such prolonged or regular surveillance of the movements of the suspects would most likely be noticed, causing them to become more cautious in their illegal activities, to flee to avoid further investigation and prosecution, to cause a real threat to the safety of the informant(s) and undercover agent(s), or to otherwise compromise the investigation.

Physical surveillance is also unlikely to establish conclusively the roles of the named conspirators, to identify additional conspirators, or otherwise to provide admissible

1

evidence in regard to this investigation because (discuss any of the following which are applicable to the case):

- the subjects are using counter-surveillance techniques, such as erratic driving behavior, or have evinced that they suspect that law enforcement surveillance is being conducted against them; and/or

- it is not possible to determine the full nature and scope of the aforementioned offenses by the use of physical surveillance; and/or

- the nature of the neighborhood forecloses physical surveillance; (e.g., close-knit community, physical location (cul-de-sac, dead-end, large apartment building), observant neighbors); and/or

- further surveillance would only serve to alert the suspects of the law enforcement interest in their activities and compromise the investigation.

Use of Grand Jury Subpoenas

Based upon your affiant's experience and conversations with Assistant United States Attorney _____, who has experience prosecuting violations of criminal law, your affiant believes that subpoenaing persons believed to be involved in this conspiracy and their associates before a Federal Grand Jury would not be completely successful in achieving the stated goals of this investigation. If any principals of this conspiracy, their co-conspirators and other participants were called to testify before the Grand Jury, they would most likely be uncooperative and invoke their Fifth Amendment privilege not to testify. It would be unwise to seek any kind of immunity for these persons, because the granting of such immunity might foreclose prosecution of the most culpable members of this conspiracy and could not ensure that such immunized witnesses would provide truthful testimony. Additionally, the service of Grand Jury subpoenas upon the principals of the conspiracy or their co-conspirators would only (further) alert them to the existence of this investigation, causing them to become more cautious in their activities, to flee to avoid further investigation or prosecution, to threaten the lives of the informant(s) and the undercover agent(s), or to otherwise compromise the investigation.

(Add specific information regarding any persons who have been subpoenaed before the Grand Jury, especially when the Fifth Amendment was invoked or when the witness later advised the targets.)

Confidential Informants and Cooperating Sources

Reliable confidential informants/cooperating sources have been developed and used, and will continue to be developed and used, in regard to this investigation. However, these sources (discuss only those that are applicable):

- exist on the fringe of this organization and have no direct contact with mid- or high-level members of the organization, or such contact is virtually impossible because the sources have no need to communicate with such individuals; and/or

- refuse to testify before the Grand Jury or at trial because of fear of personal or family safety, or their testimony would be uncorroborated or otherwise would be subject to impeachment (due to prior record, criminal involvement, etc.); and/or

- are no longer associated with the subjects of this investigation (and their information is included for historical purposes only); and/or

- are unable to furnish information which would identify fully all members of this ongoing criminal conspiracy or which would define the roles of those conspirators sufficiently for prosecution.

(In addition, discuss whether the information provided by the confidential sources, even if all sources agreed to testify, would not, without the requested electronic surveillance, result in a successful prosecution of all of the participants.)

Undercover Agents

Undercover agents have been unable to infiltrate the inner workings of this conspiracy due to the close and secretive nature of this organization. Your affiant believes that there are no undercover agents who can infiltrate the conspiracy at a level high enough to identify all members of the conspiracy or otherwise satisfy all the goals of this investigation. (Indicate if infiltration is not feasible because the confidential informant(s) is not in a position to make introductions of undercover agents to mid- or high-level members of the organization.)

(Details of the use of undercover agents should have been provided in the body of the affidavit, with this section indicating the limitations of such use.)

Interviews of Subjects or Associates

Based upon your affiant's experience, I believe that interviews of the subjects or their known associates would produce insufficient information as to the identities of all of the persons involved in the conspiracy, the source of (the drugs, financing, etc.), the location of (records, drugs, etc.), and other pertinent information regarding the named crimes. Your affiant also believes that any responses to the interviews would contain a significant number of untruths, diverting the investigation with false leads or otherwise frustrating the investigation. Additionally, such interviews would also have the effect of alerting the members of the conspiracy, thereby compromising the investigation and resulting in the possible destruction or concealment of documents and other evidence, and the possibility of harm to cooperating sources whose identities may become known or whose existence may otherwise be compromised.

(This portion of the affidavit is sometimes merged with the discussion regarding the use of the Federal Grand Jury. Any actual interviews conducted, and any resulting problems, should also be discussed here.)

Search Warrants

The execution of search warrants in this matter has been considered. However, use of such warrants would, in all likelihood, not yield a considerable quantity of (narcotics, money, or other identified contraband) or (relevant documents), nor would the searches be likely to reveal the total scope of the illegal operation and the identities of the co-conspirators. (It is unlikely that all, or even many, of the principals of this organization would be at any one location when a search warrant was executed.) The affiant believes that search warrants executed at this time would be more likely to compromise the investigation by alerting the principals to the investigation and allowing other unidentified members of the conspiracy to insulate themselves further from successful detection.

Pen Registers/Telephone Toll Records/Traps and Traces

Pen register (and/or trap and trace) information has been used in this investigation, including pen register(s) (and/or traps and traces) on the target telephone(s), as described above. The pen register (and/or trap and trace) information has verified frequent telephone communication between the target telephone(s) and other telephones. Pen registers (and/or traps and traces), however, do not record the identity of the parties to the conversation, cannot identify the nature or substance of the conversation, or differentiate between legitimate calls and calls for criminal purposes. A pen register (and/or trap and trace) cannot identify the source or sources of the controlled substances, nor can it, in itself, establish proof of the

conspiracy. Telephone toll information, which identifies the existence and length of telephone calls placed from the target telephone to telephones located outside of the local service zone, has the same limitations as pen registers (and/or traps and traces), does not show local calls, and is generally available only on a monthly basis.

Other Limitations

(Provide details concerning violence, such as murdered or hurt witnesses, threats, etc., and other situations present in your investigation that limit the effectiveness of normal investigative techniques.)

Based upon the foregoing, it is your affiant's belief that the interception of (wire)(oral) communications is an essential investigative means in obtaining evidence of the offenses in which the subject(s) and others as yet unknown are involved.

PRIOR APPLICATIONS

Based upon a check of the records of the (Federal Bureau of Investigation, the Drug Enforcement Administration, and any other appropriate agency), no prior federal applications for an order authorizing or approving the interception of wire, oral, or electronic communications have been made involving the persons, premises or facilities named herein. (If the facts warrant, include additional information concerning prior or ongoing electronic surveillance, including the dates of the interception, the jurisdiction where the order was signed and the relevance, if any, to the instant application. While there is no obligation to conduct a search of state law enforcement electronic surveillance indices, information about prior state taps must be included if the government has knowledge of them through other means.)

MINIMIZATION

All interceptions will be minimized in accordance with the minimization requirements of Chapter 119 of Title 18, United States Code, and all interceptions conducted pursuant to this Court's Order will terminate upon attainment of the authorized objectives or, in any event, at the end of thirty (30) days measured from the earlier of the day on which investigative or law enforcement officers first begin to conduct an interception under the Court's Order or ten (10) days after the Order is entered. Monitoring of conversations will terminate immediately when it is determined that the conversation is unrelated to communications subject to interception under Chapter 119 of Title 18, United States Code. Interception will be suspended immediately when it is determined through voice identification, physical surveillance, or otherwise, that none of the named interceptees or any of their confederates, when identified, are participants in the conversation, unless it is determined during

the portion of the conversation already overheard that the conversation is criminal in nature. (If pertinent, add additional language concerning the use of foreign languages and other minimization considerations particular to the case, such as targeting the use of public facilities or premises or non-interception of privileged communications of interceptees who have pending criminal charges.)

(NAME)
Special Agent
(Agency)

Sworn to before me this
_____ day of _____, 199__.

UNITED STATES DISTRICT COURT JUDGE
(District)

Order for Interception of Wire and/or Oral Communications

(FORM 3)

UNITED STATES DISTRICT COURT
DISTRICT _____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA FOR)
AN ORDER AUTHORIZING THE INTERCEPTION)
OF (WIRE) (ORAL) COMMUNICATIONS)

ORDER AUTHORIZING THE INTERCEPTION OF (WIRE)
(ORAL) COMMUNICATIONS

Application under oath having been made before me by
_____, Assistant United States Attorney,
_____ District of _____, an investigative
or law enforcement officer of the United States within the
meaning of Section 2510(7) of Title 18, United States Code, for
an Order authorizing the interception of (wire) (oral)
communications pursuant to Section 2518 of Title 18, United
States Code, and full consideration having been given to the
matter set forth therein, the Court finds:

(the following lettered paragraphs should be virtually
identical to the probable cause paragraphs contained in the
application and affidavit)

a. there is probable cause to believe that (list the
violators) have committed, and are committing, and will continue
to commit violations of (list the offenses - must be ones
enumerated in Section 2516 of Title 18, United States Code);

b. there is probable cause to believe that particular
(wire) (oral) communications of (name the interceptees) concerning
the above-described offenses will be obtained through the
interception for which authorization has herewith been applied.
In particular, there is probable cause to believe that the
interception of (wire communications to and from the telephone
bearing the number _____, subscribed to by
_____ and located at/billed to
_____) (oral communications occurring in the premises
located at _____ and/or in and around the
vehicle described as _____), will concern the
specifics of the above offenses, including the manner and means
of the commission of the offenses(s); (If roving interception is
applied for: "the application has also demonstrated adequately
within the meaning of Title 18, United States Code, Section 2518

(11)(a) and/or (b), that (if oral: "specification of the place(s) where the oral communications of (name the interceptee(s)) are to be intercepted is not practical") (if wire: "(name the interceptee(s)) use(s) various changing facilities for the purpose of thwarting electronic surveillance."));

c. it has been established that normal investigative procedures have been tried and have failed, reasonably appear to be unlikely to succeed if tried, or are too dangerous to employ; and

d. there is probable cause to believe that (identify the facilities from which, or the place where, the wire or oral communications are to be intercepted) have been and will continue to be used in connection with commission of the above-described offenses.

WHEREFORE, IT IS HEREBY ORDERED that Special Agents of the (name the investigative agency/agencies; also indicate if state and local officers are participating in the investigation, particularly if they will be monitors) are authorized, pursuant to an application authorized by a duly designated official of the Criminal Division, United States Department of Justice, pursuant to the power delegated to that official by special designation of the Attorney General and vested in the Attorney General by Section 2516 of Title 18, United States Code, to intercept (wire)(oral) communications (if wire: "to and from the above-described telephone(s)") (if oral: "in the above-described premises (or vehicle).")

PROVIDED that such interception(s) shall not terminate automatically after the first interception that reveals the manner in which the alleged co-conspirators and others as yet unknown conduct their illegal activities, but may continue until all communications are intercepted which reveal fully the manner in which the above-named persons and others as yet unknown are committing the offenses described herein, and which reveal fully the identities of their confederates, their places of operation, and the nature of the conspiracy involved therein, or for a period of thirty (30) days measured from the day on which investigative or law enforcement officers first begin to conduct an interception under this order or ten (10) days after this order is entered, whichever is earlier.

(If a mobile or cellular telephone or facility, add:

IT IS ORDERED FURTHER that in the event that the target facility/vehicle is transferred outside the territorial jurisdiction of this court, interceptions may take place in any other jurisdiction within the United States.)

(If oral communications, add:

IT IS ORDERED FURTHER that Special Agents of the (name the agency/agencies) may make all necessary surreptitious and/or forcible entries to effectuate the purposes of this order, including but not limited to entries to install, maintain and remove electronic listening devices within (describe the premises or vehicle). Applicant shall notify the Court of each surreptitious entry.)

(If interception of wire communications is requested, add:

IT IS ORDERED FURTHER that the authorization apply not only to the target telephone number(s) listed above, but to any changed telephone number subsequently assigned to the same cable, pair, and binding posts utilized by the target telephone(s) within the thirty (30) day period. (In the case of a cellular telephone: "... but to any changed telephone number or any other telephone number subsequently assigned to or used by the instrument bearing the same electronic serial number as the target cellular phone within the thirty (30) day period.") It is also ordered that the authorization apply to background conversations intercepted in the vicinity of the target telephone(s) while the telephone(s) is off the hook or otherwise in use.)

(If a roving interception is being ordered, add:

IT IS ORDERED FURTHER that the authorization to intercept (wire)(oral) communications shall include the interception of the (wire)(oral) communications of (name the interceptee(s)) ((if wire: "from various and changing telephone facilities," pursuant to 18 U.S.C. § 2518(11)(b)); (if oral: "from presently unknown premises used by (name the interceptee(s)) that it is not practical to specify, pursuant to 18 U.S.C. § 2518(11)(a)).

(If wire communications, add:

IT IS ORDERED FURTHER that, based upon the request of the Applicant pursuant to Section 2518(4) of Title 18, United States Code, the (name the communication service provider(s)), an electronic communication service provider(s) as defined in Section 2510(15) of Title 18, United States Code, shall furnish the (investigative agency) with all information, facilities and technical assistance necessary to accomplish the interceptions unobtrusively and with a minimum of interference with the services that such provider is according the persons whose communications are to be intercepted, with the service provider(s) to be compensated by the Applicant for reasonable expenses incurred in providing such facilities or assistance.)

IT IS ORDERED FURTHER that, to avoid prejudice to the government's criminal investigation, the provider(s) of the

electronic communications service and its agents and employees are ordered not to disclose or cause a disclosure of the Order or the request for information, facilities and assistance by the (investigative agency), or the existence of the investigation to any person other than those of its agents and employees who require this information to accomplish the services hereby ordered. In particular, said provider(s) and its agents and employees shall not make such disclosure to a lessee, telephone subscriber or any interceptee or participant in the intercepted communications.

IT IS ORDERED FURTHER that this order shall be executed as soon as practicable and that all monitoring of (wire)(oral) communications shall be conducted in such a way as to minimize the interception and disclosure of the communications intercepted to those communications relevant to the pending investigation. The interception of (wire)(oral) communications must terminate upon the attainment of the authorized objectives, not to exceed thirty (30) days measured from the earlier of the day on which investigative or law enforcement officers first begin to conduct an interception of this order or ten (10) days after the order is entered.

Monitoring of conversations must terminate immediately when it is determined that the conversation is unrelated to communications subject to interception under Chapter 119, Title 18, United States Code. Interception must be suspended immediately when it is determined through voice identification, physical surveillance, or otherwise, that none of the named interceptees or any of their confederates, when identified, are participants in the conversation unless it is determined during the portion of the conversation already overheard that the conversation is criminal in nature. If the conversation is minimized, the monitoring agent shall spot check to insure that the conversation has not turned to criminal matters.

IT IS ORDERED FURTHER that Assistant United States Attorney _____ or any other Assistant United States Attorney familiar with the facts of this case shall provide this Court with a report on or about the (tenth), (twentieth), and (thirtieth) days following the date of this Order showing what progress has been made toward achievement of the authorized objectives and the need for continued interception. If any of the above-ordered reports should become due on a weekend or holiday, IT IS ORDERED FURTHER that such report shall become due on the next business day thereafter.

IT IS ORDERED FURTHER that this Order, the application, affidavit and proposed order(s), and all interim reports filed with this Court with regard to this matter, shall be sealed until further order of this Court, except that copies of the order(s), in full or redacted form, may be served on the (investigative

agency/agencies) and the service provider(s) as necessary to effectuate this order.

UNITED STATES DISTRICT COURT JUDGE
(District)

Dated this _____ day of _____, 199__.

Order to Service Provider

(FORM 4)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA FOR)
AN ORDER AUTHORIZING THE INTERCEPTION)
OF (WIRE) (ELECTRONIC) COMMUNICATIONS)

ORDER TO SERVICE PROVIDER

This matter comes before the Court pursuant to the Application of the United States of America for an order authorizing the interception of (wire) (electronic) communications pursuant to Title 18, United States Code, Section 2518, (if wire: "to and from the telephone(s) bearing the number(s) _____ and located at/billed to _____") (if electronic: "to and from the pager/facsimile machine/computer bearing the telephone number and located at/billed to _____").

The Court, having reviewed the Application and found that it conforms in all respects to the requirements of Title 18, United States Code, Sections 2516 and 2518, has this day signed an Order conforming to the provisions of Title 18, United States Code, Section 2518, authorizing the (name the investigative agency/agencies) to accomplish the aforesaid interception.

IT APPEARING FURTHER that the Applicant has requested that the (name the service provider(s)) be directed to furnish, and continue to furnish, the Applicant and (name the investigative agency) with all information, facilities and technical assistance necessary to accomplish the interception(s) unobtrusively and with a minimum of interference with the services such provider(s) is according the person(s) whose communications are to be intercepted, and to ensure an effective and secure installation of electronic devices capable of interception of wire communications over the above-described telephone(s) and/or electronic communications over the above-described facsimile machine/pager/computer.

IT IS HEREBY ORDERED that the (name the service provider(s)), shall furnish, and continue to furnish, the (name the investigative agency) with all information, facilities and technical assistance necessary to accomplish the interception(s) unobtrusively and with minimum interference with the services that such provider(s) is according the person(s) whose

communications are to be intercepted, and to ensure an effective and secure installation of electronic devices capable of interception of wire communications over the above-described telephone(s) and/or facsimile machine/pager/computer.

IT IS ORDERED FURTHER that the service provider(s) is to be compensated by the Applicant for reasonable expenses incurred in providing such facilities or assistance.

IT IS ORDERED FURTHER that the furnishing of said information, facilities, and technical assistance shall terminate thirty (30) days measured from the earlier of the day that assistance is provided under this order or ten (10) days from the date this Order is entered, unless otherwise ordered by this Court; and

IT IS ORDERED FURTHER that this Order is sealed, except that copies of this Order may be served on the (name the investigative agency/agencies) and (name the service provider(s)), and, to avoid prejudice to the criminal investigation, that the (name the service provider(s)) and its agents and employees shall not disclose or cause a disclosure of this Order or the request for assistance or the existence of this investigation to any person other than those of its agents and employees who require this information to accomplish the services hereby ordered, unless and until otherwise ordered by this Court. In particular, no such disclosure may be made to a lessee, telephone subscriber, or any interceptee or participant in the intercepted communications.

DATED this _____ day of _____, 199__.

UNITED STATES DISTRICT COURT JUDGE
(District)

SAMPLE MINIMIZATION INSTRUCTIONS
FOR ORAL AND WIRE COMMUNICATIONS

(FORM 5)

MEMORANDUM

TO: Monitoring Agents
FROM: AUSA _____
RE: Minimization Instructions
DATE: _____

1. All agents must read the affidavit, application, order and these instructions and sign these instructions before monitoring.

2. The Order of _____ only authorizes the interception of conversations of (name the interceptees listed in the Order) with anyone else occurring (to and from telephone number _____ subscribed to by _____) (at the premises known as _____ and located at _____), regarding offenses involving (list the offenses).

3. Agents may spot monitor for a reasonable period not to exceed two minutes to determine whether the subject is present and participating in a conversation. This spot monitoring may occur as often as is reasonable, but in any event at least one minute should elapse between interceptions.

4. If, during this spot monitoring, it is determined that additional individuals are engaged in criminal conversation, intercepts may continue despite the fact that the named subject is not engaged in conversations, until the conversation ends or becomes non-pertinent. If individuals other than the subject are participating in criminal conversation, continue to monitor and advise the case agent or supervisor immediately. If these individuals can be identified, provide this information also.

5. If the subject is engaged in conversation, interception may continue for a reasonable time, usually not in excess of two minutes, to determine whether the conversation concerns criminal activities.

(a) If such a conversation is unclear but may be related to (name the offenses), interception may continue until such time as it is determined that the conversation clearly no longer relates to that topic.

(b) If such a conversation is unclear but may relate to other criminal activities, interception should cease after about two minutes unless it can be determined within that time that the

conversation does in fact relate to such other criminal activities, in which case interception may continue.

6. The above instructions regarding the number of minutes of permissible interception will vary once experience has been gained. If experience shows that conversations between certain people are invariably innocent, interception of such conversations should be ended sooner. If experience shows that other individuals always discuss criminal activities, a longer interception may be justified. This is especially true for individuals who can be identified as participants with the subjects in possessing and distributing controlled substances. Read all of the logs of interceptions on a continuing basis and notify the case agent if patterns develop.

7. No conversation may be intercepted that would fall under any legal privilege. The four categories of privileged communications are described below:

(a) Attorney-Client Privilege: Never knowingly listen to or record a conversation between a subject and his or her attorney when other parties are not present. Any time that an attorney is a party to a conversation, call the case agent immediately. If it is determined that a conversation involving an attorney constitutes legal consultation of any kind, notify the case agent, shut off the monitor and stop recording, unless you are able to determine from the interception of any conversation involving an attorney that third parties who are not involved in the legal matters being discussed are present. If such third parties are present, and only if they are present, may you intercept such conversations following the above-described rules of minimization. In any event, notify the case agent immediately.

(b) Parishioner-Clergyman Privilege: All conversations and conduct between a parishioner and his clergyman are to be considered privileged. An electronic surveillance order could not be obtained to listen to a subject confess his sins to a priest in a confessional booth; similarly, a subject discussing his personal, financial or legal problems with his priest, minister, rabbi, etc. may likewise not be intercepted. Thus, if it is determined that a clergyman is a party to a communication being intercepted and that the communication is penitential in nature, turn off the monitor, stop recording, and notify the case agent.

(c) Doctor-Patient Privilege: Any conversation a patient has with a doctor relating to diagnosis, symptoms, treatment, or any other aspects of physical, mental or emotional health, is privileged. If it is determined that a person is talking to his doctor and that the conversation concerns the person's health (or someone else's health), turn off the machine and notify the case agent.

(d) Husband-Wife Privilege: As a general rule, there is also a privilege covering communications between lawfully married spouses. Monitoring should be discontinued and the case agent notified if it is determined that a conversation solely between a husband and wife is being intercepted. If a third person is present, however, the communication is not privileged and that conversation may be monitored in accordance with the previously described rules of minimization. If the conversation is between the named subjects and their respective spouses, the conversation may be monitored in accordance with the previously described rules of minimization regarding monitoring these individuals' conversations to determine whether they are discussing crimes. If the nature of the conversation is criminal, monitoring may continue; otherwise, it may not be monitored.

8. Abstracts or summaries of each conversation are to be made at the time of interception and are to be included in the logs and the statistical analysis sheet. If the conversation is not recorded entirely, an appropriate notation should be made indicating the incomplete nature of the conversation and why the conversation was not recorded completely (e.g., "non-pertinent" or "privileged").

9. The logs should reflect all activity occurring at the monitoring station concerning both the intercepted conversations as well as the equipment itself (e.g., "replaced tape," "malfunction of tape recorder," "no overheard conversation"). These logs will be used ultimately to explain the monitoring agent's actions when intercepting communications. It is important to describe the parties to each conversation, the nature of each conversation, and the action taken. All monitoring agents will record the times their equipment is turned on and off.

10. All conversations that are monitored must be recorded.

11. The Log

The monitoring agents should maintain a contemporaneous log, by shifts, of all communications intercepted, indicating the reel and footage locations of each communication; the time and duration of the interception; whether outgoing or incoming in the case of telephone conversations; the number called if the call was outgoing; the participants, if known; and the subjects and a summary of the content of pertinent conversations. Any peculiarities, such as codes, foreign language used, or background sounds, should also be noted. When the interception of a communication is terminated for purposes of minimization, that fact should be noted. This log should record the names of the personnel in each shift and the function performed by each, malfunctions of the equipment or interruptions in the surveillance for any other reason and the time spans thereof, and interceptions of possibly privileged conversations or

conversations relating to crimes not specified in the original interception order. Each entry in the log should be initialed by the person making it.

12. Protection of the Recording

The following procedure should be followed during the period of authorized interceptions:

(a) Either during or at the end of each recording period, copies of the recorded conversations should be made for the use of the investigative agencies and the supervising attorney;

(b) The original recording should be placed in a sealed evidence envelope and kept in the custody of the investigative agencies until it is made available to the court at the expiration of the period of the order; and

(c) A chain of custody form should accompany the original recording. On this form should be a brief statement, signed by the agent supervising the interception, which identifies:

i - the order that authorized the recorded interceptions (by number if possible);

ii - the date and time period of the recorded conversations;

iii - the identity (when possible) of the individuals whose conversations were recorded; and

iv - the place (e.g., location of telephone) where intercepted communications took place.

(d) The form should indicate to whom the case agent has transferred the custody of the original recording and the date and time that this occurred. Each subsequent transfer, including that to the court, should be noted on the form.

(e) The case agent should mark a label attached to the original tape reel/cassette in order to identify it as corresponding with accompanying chain of custody forms. The date of the recording should also be marked on the label and this should be initialed by the agent.

(f) Each agent or other person signing the chain of custody form should be prepared to testify in court that the original tape, while in his custody, was kept secure from the access of third parties (unless noted to the contrary on the form) and was not altered or edited in any manner. It is the responsibility of the investigative agencies to ensure that original recordings in their custody will be maintained in such a way as to ensure their

admissibility in evidence at trial over objections to the integrity of the recording.

13. Procedure When No Recording Can be Made

In those unusual instances when no recording of the intercepted conversations can be made, the following procedure should be used:

(a) The monitoring agent should make a contemporaneous log or memorandum that is as near to a verbatim transcript as is possible;

(b) The log or memorandum should close with a brief statement signed by the agent indicating the date, time, and place of the intercepted conversation. The order authorizing the interception should be identified. The agent should indicate that the log or memorandum contains the contents of the intercepted communication which he overheard. This should be followed by the agent's signature; and

(c) This log should be treated by the investigative agencies as if it were an original recording of the intercepted communication.

14. If the conversation occurs in a language other than English that no one at the monitoring post understands, the entire conversation should be monitored and recorded and then minimized by a person familiar with the investigation, but who is not actively involved in it, in accordance with the minimization rules set forth above.

15. If anything appears to be breaking suddenly, please call the case agent or the AUSA. Several telephone numbers will be posted at the monitoring post.

Assistant United States Attorney

Application for Electronic Communications Interception

(FORM 6)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA FOR)
AN ORDER AUTHORIZING THE INTERCEPTION)
OF ELECTRONIC COMMUNICATIONS)

APPLICATION FOR INTERCEPTION OF ELECTRONIC COMMUNICATIONS

_____, Assistant United States Attorney,
_____ District of _____/Special Attorney, United
States Department of Justice, being duly sworn, states:

1. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, that is, an attorney authorized by law to prosecute or participate in the prosecution of United States federal felony offenses. I am also an attorney for the Government as defined in Rule 54(c) of the Federal Rules of Criminal Procedure, and, therefore, pursuant to Section 2516(3) of Title 18, United States Code, I am authorized to make an application to a Federal judge of competent jurisdiction for an order authorizing the interception of electronic communications.

2. This application is for an order pursuant to Section 2518 of Title 18, United States Code, authorizing the interception of electronic communications for a thirty (30) day period of (name the interceptees) and others as yet unknown to the (digital-display paging device(s)/facsimile machine/computer) bearing the telephone number(s) _____, subscribed to by _____, concerning federal felony offenses, that is, offenses involving violations of (list the section(s) of the United States Code and briefly describe the applicable offense(s)).

3. I have discussed all of the circumstances of the above offenses with Special Agent _____ of the _____, who has directed and conducted this investigation, and have examined the Affidavit of Special Agent _____ of this date (attached to this application as Exhibit ___, and which is incorporated by reference). Whereof your applicant states upon information and belief that:

a. there is probable cause to believe that (name the violators) have committed, are committing and will continue to commit violations of (list the offenses);

b. there is probable cause to believe that particular electronic communications of (name the interceptee(s)) concerning the above-described offenses will be obtained through the interception for which authorization is herein applied. In particular, there is probable cause to believe that the communications to be intercepted will concern the telephone numbers of associates of (name the violators) and the dates, times and places for commission of the aforementioned federal felony offenses when (name the interceptees) communicate with their co-conspirators, aiders and abettors, and other participants in the conspiracy, thereby identifying the co-conspirators and aiders and abettors of (name the violators) and others as yet unknown, their places of operation. In addition, these communications are expected to constitute admissible evidence of the above-described offenses;

c. normal investigative procedures have been tried and have failed, reasonably appear to be unlikely to succeed if tried, or are too dangerous to employ, as are described in further detail in the attached affidavit of Special Agent _____; and

d. there is probable cause to believe that (list the facilities from which, or the place where, the electronic communications are to be intercepted) are being, and will continue to be used in connection with the commission of the above-described offenses.

The attached affidavit contains a full and complete statement of facts concerning all previous applications that have been made to any judge of competent jurisdiction for authorization to intercept, or for approval of interception of wire, oral or electronic communications involving any of the same individuals, facilities, or places specified in this application.

On the basis of the allegations contained in this application and on the basis of the attached affidavit of Special Agent _____,

IT IS HEREBY REQUESTED that this Court issue an order, pursuant to the power conferred on it by Section 2518 of Title 18, United States Code, authorizing the (name the investigative agency/agencies) to intercept electronic communications to the above-described (digital display paging device, facsimile machine, computer), and providing that such interceptions not terminate automatically after the first interception that reveals the manner in which the alleged co-conspirators and others as yet unknown conduct their illegal activities, but continue until all

communications are intercepted which reveal fully the manner in which the above-named persons and others as yet unknown are committing the offenses described herein, and which reveal fully the identities of their confederates, their places of operation, and the nature of the conspiracy involved therein, or for a period of thirty (30) days measured from the day on which investigative or law enforcement officers first begin to conduct an interception under this Court's order or ten (10) days after this order is entered, whichever is earlier.

IT IS REQUESTED FURTHER that in the event that the target facility is transferred outside the territorial jurisdiction of this Court, interceptions may take place in any other jurisdiction within the United States.

IT IS REQUESTED FURTHER that this Court issue an order pursuant to Section 2518(4) of Title 18, United States Code, directing that (list the communications service provider(s)), a communication service provider as defined in Section 2510(15) of Title 18, United States Code, shall furnish, and continue to furnish, the applicant and investigative agency with all information, facilities and technical assistance necessary to accomplish the interceptions unobtrusively and with a minimum of interference with the services that such providers are according the persons whose communications are to be intercepted, and to ensure an effective and secure installation of electronic devices capable of interception of electronic communications over the above-described (digital display paging device, facsimile machine, computer), with the service provider to be compensated by the applicant for reasonable expenses incurred in providing such facilities or assistance.

IT IS REQUESTED FURTHER that, to avoid prejudice to this criminal investigation, the Court order the said providers of electronic communication service and their agents and employees not to disclose or cause a disclosure of this Court's order or the request for information, facilities and assistance by the (identify the investigative agency/agencies) or the existence of the investigation to any person other than those of their agents and employees who require said information to accomplish the services hereby requested. In particular, said providers and their agents and employees should be ordered not to make such disclosure to a lessee, telephone subscriber, or any interceptee or participant in the intercepted communications.

IT IS REQUESTED FURTHER that this Court direct that this order be executed as soon as practicable after it is signed and that all monitoring of communications shall be recorded and examined by monitoring agents or attorneys to determine the relevance of the intercepted electronic communications to the pending investigation and that the disclosure of the contents or nature of the electronic communications intercepted be limited to those communications relevant to the pending investigation, in

accordance with the minimization requirements of Chapter 119 of Title 18, United States Code. The interception of communications authorized by this Court's order must terminate upon attainment of the authorized objectives or, in any event, at the end of thirty (30) days measured from the earlier of the day on which investigative or law enforcement officers first begin to conduct an interception under this Court's order or ten (10) days after the order is entered, whichever is earlier.

IT IS REQUESTED FURTHER that the Court order that either Assistant United States Attorney/Special Attorney _____, or any other Assistant United States Attorney/Special Attorney familiar with the facts of this case, provide to the Court a report on or about the (tenth), (twentieth) and (thirtieth) days following the date of this order showing what progress has been made toward achievement of the authorized objectives and the need for continued interception. If any of the aforementioned reports should become due on a weekend or holiday, IT IS REQUESTED FURTHER that such report become due on the next business day thereafter.

IT IS REQUESTED FURTHER that the Court order that its orders, this application and the accompanying affidavit and proposed order(s), and all interim reports filed with the Court with regard to this matter be sealed until further order of this Court, except that copies of the order(s), in full or redacted form, may be served on the (identify the investigative agency/agencies) and the service provider(s) as necessary to effectuate the Court's order as set forth in the proposed order(s) accompanying this application.

DATED this _____ day of _____, 199__.

Assistant United States Attorney

SUBSCRIBED and SWORN to before me
this _____ day of _____, 199__.

UNITED STATES DISTRICT COURT JUDGE
(District)

Affidavit for Electronic Communications Interception

(FORM 7)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING THE)
INTERCEPTION OF ELECTRONIC)
COMMUNICATIONS)

MISC. NO.

AFFIDAVIT IN SUPPORT OF APPLICATION

_____, being duly sworn, deposes and states
as follows:

1. I am a Special Agent with the _____,
United States Department of Justice. I have been so employed by
the _____ for the past _____ () years.
I have participated in investigations involving (organized
crime/drug trafficking, etc.) activities for the past
_____ () years.

(Describe present assignment)

2. I am an investigative or law enforcement officer of the
United States within the meaning of Section 2510(7) of Title 18,
United States Code, in that I am empowered by law to conduct
investigations and to make arrests for federal felony offenses.

3. This affidavit is submitted in support of an application
for an order authorizing the interception of electronic
communications occurring (specify the facility or facilities to
which the application and affidavit are directed).

4. I have participated in the investigation of the above
offenses. As a result of my personal participation in this
investigation, through interviews with and analysis of reports
submitted by other (Special Agents of the _____ and/or
other state/local law enforcement personnel), and by the analysis
of (surveillance logs/pen register information, etc.), I am
familiar with all aspects of this investigation. On the basis of
this familiarity, and on the basis of other information which I
have reviewed and determined to be reliable, I allege that:

a. there is probable cause to believe that (list the
violators) have committed, are committing, and will continue

to commit (list the offense(s) - can be any federal felony offense).

b. there is probable cause to believe that particular electronic communications of (list the interceptees) concerning the above offenses will be obtained through the interception of such communications to the (digital pager/facsimile machine assigned telephone number(s) _____, subscribed to by _____, (and, if applicable, the facility's physical location)). In particular, there is probable cause to believe that the communications to be intercepted will concern the telephone numbers of associates of (list the violator(s)) and the dates, times and places for commission of the aforementioned federal felony offenses when (list the interceptees) communicate with their co-conspirators, aiders and abettors, and other participants in the conspiracy, thereby identifying the co-conspirators and aiders and abettors of (the violators), and others as yet unknown, their places of operation, (etc.). In addition, these communications are expected to constitute admissible evidence of the above-described offenses.

c. normal investigative procedures have been tried and have failed, reasonably appear to be unlikely to succeed if tried, or are too dangerous to employ, as is described herein in further detail.

d. there is probable cause to believe that (list the facilities over which the electronic communications are to be intercepted) are being, and will continue to be, used in connection with the commission of the above offenses.

PERSONS EXPECTED TO BE INTERCEPTED

Include a short description of each expected interceptee; if appropriate, explain why certain participants in the offenses are not expected to be interceptees.

FACTS AND CIRCUMSTANCES

Provide an in-depth discussion of the facts in support of the probable cause statements above. If informant information provides a basis for any of the probable cause for any of the required information, provide adequate qualifying language for each informant.

(In drug cases, if appropriate, include a "facts and circumstances" paragraph regarding use of pagers, e.g., "I know from my training, experience, and discussions with other experienced agents that narcotics traffickers frequently use paging devices to further their illicit business. Pagers permit co-conspirators to contact each other with virtually no possibility that their communications will be intercepted. For

example, the type of paging device used in this matter allows a conspirator to signal a confederate, identify himself through a numerical code, and convey the number of a secure or non-suspect telephone, usually a pay telephone, at which he can be contacted. The conspirator receiving this information can then go to a secure or non-suspect telephone, return the call, and engage in a criminal discussion with his confederate which, under normal circumstances, will be incapable of interception by law enforcement authorities.")

NORMAL INVESTIGATIVE PROCEDURES

Need for Electronic Interception

Based upon your affiant's training and experience, as well as the experience of other (list the Special Agents of the _____ and/or state/local officers of _____), and based upon all of the facts set forth herein, it is your affiant's belief that the interception of electronic communications is the only available technique with a reasonable likelihood of securing the evidence necessary to prove beyond a reasonable doubt that (list the violator(s)), and others as yet unknown are engaged in the above-described offenses.

Numerous investigative procedures that are usually employed in the investigation of this type of criminal case have been tried and have failed, reasonably appear to be unlikely to succeed if they are tried, or are too dangerous to employ.

(Include a discussion of the details of specific problems regarding the use of alternative investigative techniques in this investigation. Then discuss the standard problem areas, as synopsized below, modifying the statements to comport with the actual circumstances of your case.)

Physical Surveillance

Physical surveillance has been attempted on many occasions in this investigation. Although it has proven valuable in identifying some of the targets' activities and associates, physical surveillance, if not used in conjunction with other techniques, including electronic surveillance, is of limited value. Even if highly successful, physical surveillance does not always succeed in gathering evidence of the criminal activity under investigation. It is an investigative technique used to confirm meetings between alleged conspirators, and usually only leads investigators to speculate as to the purpose of the meeting(s). It is also a technique used to corroborate information obtained from confidential informants. Further, physical surveillance of the alleged conspirators will not establish conclusively the elements of the subjects' violations and has not and most likely will not establish conclusively the identities of various conspirators. Prolonged or regular

physical surveillance of the targets would most likely be noticed, causing them to become more cautious in their illegal activities, to flee to avoid further investigation and prosecution, to cause a threat to the safety of the informant(s) and undercover agent(s), or otherwise to compromise the investigation.

With regard to this investigation, physical surveillance is unlikely to establish conclusively the roles of the named conspirators, to identify additional conspirators, to identify the conspirators' sources of supply, or otherwise to provide admissible evidence in regard to this investigation because (provide details of any of the following, as applicable):

- conspirators are using counter-surveillance, such as erratic driving behavior in order to detect surveillance; or have evinced that they suspect law enforcement surveillance of their activities;

- the nature of the neighborhood forecloses physical surveillance (e.g., a close-knit community; cul-de-sac, dead end, or large apartment building; and/or the neighbors all know each other and call the police when surveillance is spotted);

- further surveillance would only serve to alert the conspirators of the law enforcement interest in their activities and compromise the investigation.

Use of Grand Jury Subpoenas

Based upon your affiant's experience and conversations with Assistant United States Attorneys for the _____ District of _____ who have experience prosecuting violations of criminal law, your affiant believes that subpoenaing persons who are believed to be involved in this conspiracy, or their associates before a Federal Grand Jury would most likely not be completely successful in achieving the stated goals of this investigation. The targets of this investigation, and their co-conspirators and other participants, should they be called to testify before the Grand Jury, would most likely be uncooperative and invoke their Fifth Amendment privilege not to testify. It would then be unwise to seek any kind of immunity for any of these persons because the granting of such immunity might foreclose prosecution of the most culpable members of this conspiracy, and could not ensure that such immunized witnesses would provide truthful testimony before the Grand Jury. Additionally, the service of Grand Jury subpoenas upon the targets or their co-conspirators would only alert the targets to the existence of this investigation, thereby causing them to become more cautious in their activities, to flee to avoid further investigation or prosecution, to threaten the lives of

the informant(s) and the undercover agent(s), or otherwise to compromise this investigation.

(Add specific information about any persons who have been subpoenaed before the Grand Jury, especially when the Fifth Amendment was invoked or when the witness later advised the targets.)

Confidential Informants and Cooperating Sources

Reliable confidential informants/cooperating sources have been developed and used, and will continue to be developed and used, in regard to this investigation, but these sources (discuss those that are applicable):

- exist on the fringe of this organization and, therefore, have no direct contact with mid- or high-level members of the organization; or such contact is virtually impossible because the sources have no need to communicate with such individuals;

- refuse to testify before the Grand Jury or at trial because of a fear for personal or family safety; or their testimony would be uncorroborated or otherwise subject to impeachment (due to prior record, criminal involvement, etc.);

- are no longer associated with the targets of this investigation and their information is included for historical purposes only.

None of the confidential informants described in this affidavit are able to furnish information that would identify fully all members of this ongoing criminal conspiracy or define the roles of those conspirators sufficiently for prosecution or that would identify sufficiently (the source(s) of supply or all details of delivery, quantities, financial arrangements, and the like), etc.

Your affiant believes that information provided by the confidential sources, even if all sources agreed to testify, would not, without the evidence available through the requested electronic surveillance, result in a successful prosecution of all of the participants.

Undercover Police Officers and Agents

Undercover police officers and/or agents have been unable to infiltrate the inner workings of this conspiracy due to the close and secretive nature of this organization. Your affiant believes that there are no undercover officers/agents who can infiltrate the conspiracy at a level high enough to identify all members of the conspiracy or otherwise satisfy all the goals of this

investigation. (Indicate if infiltration is not feasible because the confidential informant(s) is not in a position to make introductions of undercover officers to mid- or high-level members of the organization.)

(Details of the use of undercover officers should have been provided in the body of this affidavit, with this section indicating the limitations of such usage.)

Interviews of Subjects or Associates

Based upon your affiant's experience, your affiant believes that interviews of subjects or their known associates would produce insufficient information concerning the identities of all of the persons involved in the conspiracy, the source of the drugs, financing, etc., the location of records, drugs, etc., or other pertinent information regarding the subject crimes. Your affiant also believes that any responses to the interviews would contain a significant number of half-truths and untruths, diverting the investigation with false leads or otherwise frustrating the investigation. Additionally, such interviews would likely result in non-targeted interviewees alerting the members of the conspiracy, thereby compromising the investigation and resulting in the possible destruction or concealment of (documents) (other evidence) and the possibility of harm to cooperating source(s), the identity of whom may become known or whose existence may otherwise be compromised.

(This portion of the affidavit is sometimes merged with the discussion regarding the use of the Federal Grand Jury. Any actual interviews conducted, and any resulting problems should also be discussed here.)

Search Warrants

The execution of search warrants in this matter has been considered. However, use of such warrants would, in all likelihood, not yield a considerable quantity of narcotics or relevant documents, nor would the searches conducted pursuant to such warrants be likely to reveal the total scope of the criminal operation and the identities of the co-conspirators. (It is unlikely that all, or even many, of the principals of this organization would be at any one location when a search warrant was executed.) Your affiant believes that search warrants executed at this time would be more likely to compromise the investigation by alerting the principals of the investigation, thereby, allowing unidentified co-conspirators to insulate themselves further from successful detection, as well as to otherwise frustrate the purposes of this investigation. (If search warrants were executed, then discuss the results and why this information is not enough to satisfy the goals of the investigation.)

Pen Registers/Telephone Tolls/Trap and Trace

Telephone toll/pen register/trap and trace information has been used in this investigation, as described above. (Provide a synopsis of the results obtained from a review of these phone records; describe why this information is insufficient to identify fully other coconspirators or fulfill the needs of the investigation.)

Other Limitations

(Provide details as to violence (murdered or hurt witnesses, threats, etc.) and other situations present in this investigation that limit the effectiveness of normal investigative techniques.)

Based upon the foregoing, it is your affiant's belief that the interception of electronic communications is an essential investigative means in obtaining evidence of the totality of the offenses in which the subject(s) and others as yet unknown are involved.

PRIOR APPLICATIONS

Based upon a check of the records of the Federal Bureau of Investigation, (and any other pertinent agency) no prior applications for an order authorizing the interception of wire, oral or electronic communications have been made involving the persons, premises or facilities named herein. If the facts warrant, include additional information concerning prior or ongoing electronic surveillance, (person named, court that issued the order, date and relevance, if any, to the current investigation.)

MINIMIZATION

Suggested language for pagers:

All monitoring of electronic communications of the digital-display paging device assigned telephone number () _____, will be recorded and examined by monitoring agents and attorneys to determine their relevance to the pending investigation. The disclosure of the contents or nature of the communications intercepted over the digital-display paging device will be limited to those communications relevant to the pending investigation, in accordance with the minimization requirements of Chapter 119 of Title 18, United States Code.

Suggested language for facsimile machines:

All interceptions will be minimized in accordance with Chapter 119 of Title 18, United States Code. Fax transmissions sent or received by _____ will be minimized as follows:

each fax transmission will be printed on the machine used to intercept fax communications. The monitoring agent and AUSA will decide, based on the identities of the sender and recipient and the subject matter of the transmission, whether the fax appears to be pertinent to the criminal offenses listed in the court's order. If the fax does not appear to be pertinent, the intercepted transmission will be placed in an envelope and sealed. It will then be placed in a locked drawer until it is turned over to the court with the other intercepted transmissions after the interception order has expired. (If the facsimile machine is a dedicated to fax transmissions only or, if the facsimile machine is attached to a telephone, but the government has not applied for authorization to intercept wire communications over the telephone, then add: "It is not the intention of the Government to intercept wire communications during this investigation; only electronic communications will be intercepted.")

Because of the type of information intercepted, i.e., typewritten fax communications and not verbal communications, the monitors will be unable to minimize any non-pertinent information until after it has been received at the monitoring location. It is anticipated that the monitoring location will not be staffed at all times, but will be activated electronically. The monitoring location will be kept secure and access will be available only to persons authorized to be involved with this investigation.

CONCLUSION

Your affiant believes that the facts alleged herein establish that the targets of this investigation are engaged in an ongoing criminal enterprise and that the evidence sought will be intercepted on a continuing basis following the first receipt of the particular communications that are the object of this request. Therefore, it is requested that the interception not be required to terminate when the communications described herein are first intercepted, but be allowed to continue until communications are intercepted which fully reveal the scope of the enterprise, including the identities of all participants, their places and methods of operation, and the various criminal activities in which they are engaged which are in furtherance of

the enterprise, not to exceed thirty (30) days measured from the earlier of the day on which investigative or law enforcement officers first begin to conduct an interception under this Court's Order or ten (10) days after the Order is entered.

(NAME)
Special Agent
(Agency)

Sworn to before me this
_____ day of _____, 199_.

UNITED STATES DISTRICT COURT JUDGE
(District)

Order for Interception of Electronic Communications

(FORM 8)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA FOR
AN ORDER AUTHORIZING THE INTERCEPTION
OF ELECTRONIC COMMUNICATIONS

ORDER AUTHORIZING THE INTERCEPTION OF
ELECTRONIC COMMUNICATIONS

Application under oath having been made before me by
_____, Assistant United States Attorney, _____
District of _____/Special Attorney, United States
Department of Justice, an "investigative or law enforcement
officer" of the United States within the meaning of Section
2510(7) of Title 18, United States Code, and an attorney for the
Government as defined in Rule 54(c) of the Federal Rules of
Criminal Procedure, for an Order authorizing the interception of
electronic communications pursuant to Section 2518 of Title 18,
United States Code, and full consideration having been given to
the matter set forth therein, the Court finds:

a. there is probable cause to believe that (list the
violators) have committed, are committing, and will continue to
commit violations of (list the offenses - can be any federal
felony offense);

b. there is probable cause to believe that particular
electronic communications of (list the interceptees) concerning
the above-described offenses will be obtained through the
interception for which authorization is herein applied. In
particular, there is probable cause to believe that the
communications to be intercepted will concern the telephone
numbers of associates of (the violator(s)) and the dates, times,
and places for commission of the aforementioned federal felony
offenses when (list the interceptee(s)) communicate with their
co-conspirators, aiders and abettors and other participants in
the conspiracy, thereby identifying the co-conspirators and
others as yet unknown, their places of operation, (etc.). In
addition, these communications are expected to constitute
admissible evidence of the above-described offenses;

c. It has been established adequately that normal investigative procedures have been tried and have failed, reasonably appear to be unlikely to succeed if tried, or are too dangerous to employ;

d. there is probable cause to believe that (list the facilities over which the electronic communications are to be intercepted) have been, are being and will continue to be used in connection with the commission of the above-described offenses.

WHEREFORE, IT IS HEREBY ORDERED that Special Agents of the (name the investigative agency/agencies) are authorized to intercept electronic communications over the above-described facilities.

PROVIDED that such interception(s) shall not terminate automatically after the first interception that reveals the manner in which the alleged co-conspirators and others as yet unknown conduct their illegal activities, but may continue until all communications are intercepted which fully reveal the manner in which the above-named persons and others as yet unknown are committing the offenses described herein, and which reveal fully the identities of their confederates, their places of operation, and the nature of the conspiracy involved therein, or for a period of thirty (30) days measured from the day on which investigative or law enforcement officers first begin to conduct an interception under this Order or ten (10) days after this Order is entered, whichever is earlier.

IT IS ORDERED FURTHER that, pursuant to 18 U.S.C. § 2518(3), in the event that the target facility is transferred outside the territorial jurisdiction of this court, interceptions may take place in any other jurisdiction within the United States.

IT IS ORDERED FURTHER that, based upon the request of the Applicant pursuant to Section 2518(4) of Title 18, United States Code, (name the communication service provider(s)), communication service provider(s) as defined in Section 2510(15) of Title 18, United States Code, shall furnish, and continue to furnish, the Applicant and the investigative agency/agencies with all information, facilities, and technical assistance necessary to accomplish the interceptions unobtrusively and with a minimum of interference with the services that such provider(s) is according the persons whose communications are to be intercepted, with the service provider(s) to be compensated by the Applicant for reasonable expenses incurred in providing such facilities or assistance.

IT IS ORDERED FURTHER that, to avoid prejudice to the Government's criminal investigation, the above provider(s) of electronic communication service and its agents and employees are ordered not to disclose or cause a disclosure of this Order or the request for information, facilities, and assistance by the

(name the investigative agency/agencies) or the existence of the investigation to any person other than those of its agents and employees who require said information to accomplish the services hereby ordered. In particular, said provider(s) and its agents and employees shall not make such disclosure to a lessee, telephone or paging device subscriber or any interceptee or participant in the intercepted communications.

IT IS ORDERED FURTHER that this Order shall be executed as soon as practicable and that all monitoring of the communications shall be recorded and examined by the monitoring agents or attorneys to determine the relevance of the intercepted electronic communications to the pending investigation and that the disclosure of the contents or nature of the electronic communications intercepted be limited to those communications relevant to the pending investigation, in accordance with the minimization requirements of Chapter 119 of Title 18, United States Code. The interception of communications must terminate upon the attainment of the authorized objectives, not to exceed thirty (30) days measured from the earlier of the day on which investigative or law enforcement officers first begin to conduct an interception under this Order or ten (10) days after the Order is entered.

IT IS ORDERED FURTHER that Assistant United States Attorney/Special Attorney _____ or any other Assistant United States Attorney/Special Attorney familiar with the facts of this case shall provide this Court with a report, on or about the (tenth), (twentieth) and (thirtieth) days following the date of this Order showing what progress has been made toward achievement of the authorized objectives and the need for continued interception. If any of the above-ordered reports should become due on a weekend or holiday, IT IS ORDERED FURTHER that such report shall become due on the next business day thereafter.

IT IS ORDERED FURTHER that this Order, the application, affidavit, and proposed Order(s), and all interim reports filed with this Court with regard to this matter shall be sealed until further order of this Court, except that copies of the Order(s), in full or redacted form, may be served on the (investigative agency/agencies) and the service provider(s) as necessary to effectuate this Order.

UNITED STATES DISTRICT COURT JUDGE
(District)

DATED this _____ day of _____, 199__.

Application for Sealing

(FORM 9)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING THE)
INTERCEPTION OF (WIRE) (ORAL))
(ELECTRONIC) COMMUNICATIONS OCCURRING)
TO AND FROM (TELEPHONE NUMBER _____))
SUBSCRIBED TO BY _____)
_____.) (THE PREMISES KNOWN)
AS _____, LOCATED AT _____)
_____.) (THE FACSIMILE)
MACHINE/PAGER BEARING NUMBER _____)
_____ AND SUBSCRIBED TO BY _____)
_____.)
_____)

SEALING APPLICATION

The UNITED STATES OF AMERICA, by Assistant United States Attorney _____, herein applies for an Order:

(a) Sealing _____ reel-to-reel tape recordings (or cassette tape recordings or computer printouts) of (wire) and/or (oral) and/or (electronic) communications intercepted between _____ and _____, pursuant to the Order of this Court dated _____, (occurring to and from (telephone number _____ subscribed to by _____ and located at/billed to _____) (the premises known as _____ and located at _____);

(b) Directing that the aforementioned reel-to-reel tapes (or cassette tape recordings or computer printouts) be held in the custody of the (name the investigative agency, e.g. Federal Bureau of Investigation) for a period of ten (10) years from the date of this Order in a manner so as to prevent editing, alteration and/or destruction;

(c) Directing that the contents of the said reel-to-reel tapes (or cassette tape recordings or computer printouts) be disclosed only upon the order of this Court or any other Court of competent jurisdiction, except that disclosure may be made to other law enforcement agencies pursuant to Title 18, United States Code, Section 2517;

(d) Postponing the notification requirements of Title 18, United States Code, Section 2518(d) as to all parties intercepted during the subject electronic surveillance until further order of this Court; and

(e) Directing that this Order and Application be sealed until further order of this Court.

In support of the Application, the UNITED STATES OF AMERICA represents as follows:

1. On _____, the (name the investigative agency) applied for an Order from this Court authorizing the interception of (wire) (oral) (electronic) communications occurring to and from (telephone number, subscribed to by _____) (the premises known as _____, and located at _____). The application for authorization to intercept communications (over said telephone number) (at said premises) was supported by probable cause to believe that (name the subjects) and others have been and are committing (a) offenses involving the importation, possession with intent to distribute and distribution of narcotic drug controlled substances, conspiracy to do the same, attempts to do the same, and use of wire facilities to facilitate the same, in violation of Sections _____, Title _____, United States Code; and that evidence of said violations would be obtained through the interception of the subject (wire) (oral) (electronic) communications.

2. The requested Order was granted on _____, and authorized electronic surveillance (over the subject telephone/facsimile machine/pager) (at the subject premises) for a period of thirty (30) days. Surveillance began on _____, and continued until _____.

3. The investigation of the named subjects, as well as others who are believed to be associated with the subjects is continuing. Accordingly, notification to the parties whose communications were intercepted would alert the subjects to the existence and extent of the investigation.

WHEREFORE, I respectfully request that the Court issue an Order granting this Application.

Assistant United States Attorney

Order for Sealing

(FORM 10)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

)
IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING THE)
INTERCEPTION OF (WIRE COMMUNICATIONS)
OCCURRING TO AND FROM TELEPHONE NUMBER)

)
SUBSCRIBED TO BY)
_____) (ORAL)
COMMUNICATIONS WITHIN THE PREMISES KNOWN)
AS _____, LOCATED AT _____)
_____.) (ELECTRONIC COMMUNICA-)
TIONS OVER THE FACSIMILE MACHINE/PAGER)
BEARING NUMBER _____ AND SUBSCRIBED)
TO BY _____.))
_____)

ORDER

Upon consideration of the attached application of the UNITED STATES OF AMERICA, by Assistant United States Attorney _____, and upon finding that disclosure of the subject electronic surveillance would interfere with an ongoing criminal investigation, and also upon finding that the motion of the UNITED STATES OF AMERICA is made in good faith, it is hereby:

ORDERED

1. That _____ reel-to-reel tape recordings (or cassette tapes or computer printouts) of (wire) (oral) (electronic) communications intercepted between _____ and _____, pursuant to the Order of this Court dated _____, (occurring to and from the telephone number _____, subscribed to by _____) (within the premises known as _____, and located at _____) be sealed;
2. That the aforementioned reel-to-reel tapes (or cassette tapes or computer printouts) be held in the custody of the (name the investigative agency) for a period of ten (10) years from the date of this Order in a manner so as to prevent editing, alteration and/or destruction;
3. That the contents of the said reel-to-reel tapes (or cassette tapes or computer printouts) be disclosed only upon the order of this Court or any other Court of competent jurisdiction,

except that disclosure may be made to other law enforcement agencies pursuant to Title 18, United States Code, Section 2517;

4. That the notification requirements to Title 18, United States Code, Section 2518(d) be postponed as to all parties intercepted during the subject electronic surveillance until further order of this Court; and

5. That this Order and Application be sealed until further order of this Court.

UNITED STATES DISTRICT COURT JUDGE
(District)

(Altered to reflect 10/25/94 amendments to 18 U.S.C. § 2703'

Application for a 18 U.S.C. § 2703(d) Court Order

(FORM 11)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

)
IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER PURSUANT TO 18 U.S.C.)
§ 2703(d) DIRECTING (NAME THE)
PROVIDER OF ELECTRONIC COMMUNICATIONS))
SERVICES) TO DISCLOSE THE NAME,)
ADDRESS, TELEPHONE TOLL BILLING)
RECORDS, TELEPHONE NUMBER OR OTHER)
SUBSCRIBER NUMBER OR IDENTITY,)
LENGTH OF SERVICE, TYPES OF SERVICES,)
RECORDS OR OTHER INFORMATION RELATED)
TO TELEPHONE NUMBER(S) _____)
_____) (NAME AND ADDRESS OF)
SUBSCRIBER OR CUSTOMER))
_____)

APPLICATION

_____, an attorney of the United States Department of Justice (an Assistant United States Attorney), hereby applies to the court for an order, pursuant to 18 U.S.C. § 2703(d), directing (name the provider of services) to disclose (indicate the name, address, telephone toll billing records (enter time period sought), telephone number or other subscriber number or identity, length of service, types of services, other information (not including the contents of communications)) related to (telephone number(s) _____) (name and address of subscriber or customer). In support of this application, I state the following:

I am an attorney for the Government as defined in Rule 54(c) of the Federal Rules of Criminal Procedure and, therefore, pursuant to Section 2703(c) of Title 18, United States Code, may apply for an order as requested herein.

I certify that the (name the investigative agency/agencies) is conducting a criminal investigation in connection with possible violation(s) of (list the principal violations); that it is believed that the subjects of the investigation are using telephone number(s) _____ (listed in the name of or leased to _____) and located at (identify the location)

in furtherance of the subject offenses; and that the telephone toll billing records and other information sought are relevant and material to an ongoing criminal investigation. (Offer specific and articulable facts showing that there are reasonable grounds for such a belief).

Wherefore, the applicant requests that the court issue an order pursuant to 18 U.S.C. § 2703(d) directing (name the service provider) to provide the requested (name, address, telephone toll billing records (enter time period sought), telephone number or other subscriber number or identity, length of service, types of services, record or other information (not including the contents of communications)) related to (telephone number(s) _____) (name and address of subscriber or customer) forthwith.

I request further that this application and order be sealed by the court until such time as the court directs otherwise since disclosure at this time would seriously jeopardize the investigation.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on _____, 19____

Applicant's Signature

Title

(Altered to reflect 10/25/94 amendments to 18 U.S.C. § 2703)

18 U.S.C. § 2703(d) Court Order

(FORM 12)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

)
IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER PURSUANT TO 18 U.S.C.)
§ 2703(d) DIRECTING (PROVIDER OF)
ELECTRONIC COMMUNICATIONS SERVICES))
TO DISCLOSE (THE NAME, ADDRESS,)
TELEPHONE TOLL BILLING RECORDS,)
TELEPHONE NUMBER OR OTHER SUBSCRIBER)
NUMBER OR IDENTITY, LENGTH OF)
SERVICE, TYPES OF SERVICES))
RELATED TO (TELEPHONE NUMBER(S))
_____) (NAME AND ADDRESS OF)
SUBSCRIBER OR CUSTOMER))
_____)

ORDER

This matter having come before the court pursuant to an application under Title 18, United States Code, Section 2703(c) by _____, an attorney for the Government, which application requests an order under Title 18, United States Code, Section 2703(d) directing (name the provider(s) of service) to disclose (name, address, telephone toll billing records (enter time period), telephone number or other subscriber number or identity, length of service, types of services, other information (not including the contents of communications)) related to (telephone number(s) _____) (name and address of subscriber or customer), the court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that disclosure to any person of this investigation or this application and order entered in connection therewith would seriously jeopardize the investigation;

IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d) that (name the provider(s) of services) will, forthwith, turn over to agents of (name the investigative agency/agencies) the (name, address, telephone toll billing

records (enter time period sought), telephone number or other subscriber number or identity, length of service, types of services, record or other information (not including the contents of communications)) related to (telephone number(s) _____) (name and address of subscriber or customer).

IT IS FURTHER ORDERED that the application and this order are sealed until otherwise ordered by the court, and that (name the service provider(s)) shall not disclose the existence of this application and order of the court, or the existence of the investigation, to the listed subscriber or lessee or to any other person unless and until authorized to do so by the court.

DATED: _____

UNITED STATES MAGISTRATE
DISTRICT

Application for Trap and Trace/Pen Register

(FORM 13)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

)
IN THE MATTER OF THE)
APPLICATION OF THE)
UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING)
THE INSTALLATION AND USE)
OF A (PEN REGISTER))
(TRAP AND TRACE DEVICE))

APPLICATION

_____, an attorney of the United States Department of Justice, being duly sworn, hereby applies to the Court for an order authorizing the installation and use of a (pen register) (trap and trace device) on telephone number(s) _____. In support of this application, I state the following:

1. Applicant is an "attorney for the Government" as defined in Rule 54(c) of the Federal Rules of Criminal Procedure, and, therefore, pursuant to Section 3122 of Title 18, United States Code, may apply for an order authorizing the installation of a (trap and trace device) (pen register).

2. Applicant certifies that the (name the investigative agency) is conducting a criminal investigation of (name targets) and others as yet unknown, in connection with possible violations of (list the violations); it is believed that the subjects of the investigation are using telephone number(s) _____, (listed in the name of) (leased to) _____ and located at _____, in furtherance of the subject offenses; and that the information likely to be obtained from the (pen register) (trap and trace device) is relevant to the ongoing criminal investigation, in that, it is believed that this information will concern the aforementioned offenses.

3. Applicant requests that the Court issue an order authorizing the installation and use of (a pen register to record or decode electronic or other impulses which identify the numbers dialed or otherwise transmitted on) (and) (a trap and trace device to capture the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted to) telephone number(s) _____, and the date, time and

duration of such (incoming) (outgoing) impulses for a period of (enter the time period, not to exceed 60) days.

4. The applicant requests further that the order direct that (name the communications service provider(s)) furnish agents of the (name the investigative agency/agencies) forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the (pen register) (trap and trace device), including (installation of Caller ID service on telephone number(s) _____ and) the installation and operation of the device(s), unobtrusively and with minimum interference to the services that are accorded persons whose telephone(s) is/are to be the subject of the device(s). The communications service provider shall be compensated by the applicant for reasonable expenses incurred in providing such facilities and technical assistance.

5. The applicant requests further that the order direct that the results of the (trap and trace device) (pen register) shall be furnished to Special Agents of the (investigative agency/agencies) at reasonable intervals during regular business hours for the duration of the order.

6. The applicant requests further that the Court's order direct (name the communications service provider(s)), and its agents and employees not to disclose to the subscriber, or any other person, the existence of this order, the (pen register) (trap and trace device), or this investigation unless or until otherwise ordered by the court.

7. [Prosecutors should discuss with their agents whether, per the language of 18 U.S.C. § 3121(c), appropriate technology has become reasonably available, and then adjust the following language, accordingly.] With regard to the limitation in 18 U.S.C. § 3121(c) that the (investigative agency/agencies) shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing, the (name the investigative agency/agencies) does not believe that such technology exists.

(In the case of a trap and trace)

8. The applicant further requests that the Court's order be limited in the following respects:

- (a) the tracing operation shall be limited to (Electronic Switching Systems (ESS)) or (No. 5 cross-bar switching facilities); and
- (b) the tracing operation shall be restricted to tracing and recording only those incoming numbers originating from (identify the geographical area).

WHEREFORE, it is respectfully requested that the Court grant an order for (enter time period, not to exceed 60) days (1) authorizing the installation and use of (a pen register to record or decode electronic or other impulses which identify the numbers dialed or otherwise transmitted on) (and/or) (a trap and trace device to capture the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted to) telephone number(s) _____, (2) directing the (identify the communications service provider(s)) to forthwith furnish agents of the (name the investigative agency) with all information, facilities and technical assistance necessary to accomplish the installation of the (trap and trace device) (pen register), including installation and operation of the device(s), unobtrusively and with minimum interference to the service presently accorded the person(s) whose telephone(s) is/are to be the subject of the device(s), (3) directing the (name the service provider(s)) and its agents and employees not disclose to the subscriber or any other person the existence of the Court's order, (trap and trace device) (pen register) or this investigation unless or until otherwise ordered by the Court, and (4) sealing the application and the Court's order.

I declare under penalty of perjury that the foregoing is true and correct.

EXECUTED ON _____, 19____

Applicant

Order for Trap and Trace/Pen Register

(FORM 14)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

)
IN THE MATTER OF THE)
APPLICATION OF THE)
UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING)
THE INSTALLATION AND USE)
OF A (PEN REGISTER))
(TRAP AND TRACE DEVICE))

ORDER

This matter having come before the Court pursuant to an application under oath pursuant to Title 18, United States Code, Section 3122 by _____, an attorney for the Government, which requests an order under Title 18, United States Code, Section 3123, authorizing the installation and use of a (pen register) (trap and trace device) on telephone number(s) _____, the Court finds that the applicant has certified that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation into possible violations of (list the violations) by (list the targets) and others as yet unknown.

IT APPEARING that the information likely to be obtained by a (pen register) (trap and trace device) installed on telephone number(s) _____, (subscribed to by) (leased by) _____, and located at _____, is relevant to an ongoing criminal investigation of the specified offenses,

IT FURTHER APPEARING that [conform to application statement] with regard to the limitation in 18 U.S.C. § 3121(c) concerning pen register technology, the (name the investigative agency/agencies) does not have technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing.

IT IS ORDERED, pursuant to Title 18, United States Code, Section 3123, that agents of (name the investigative agency/agencies) may direct (list the communications service provider(s)) to install a (pen register) (and/or) (trap and trace device) on telephone number(s) _____ (to record or decode electronic or other impulses which identify the numbers

dialed or otherwise transmitted on telephone number(s) _____) (and/or) (to capture the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted to telephone number(s) _____) and the date, time, and duration of such (incoming) (outgoing) impulses for a period of (enter the time period, not to exceed 60) days; and

IT IS ORDERED FURTHER, pursuant to Title 18, United States Code, Section 3123(b)(2), that (name the communications service provider(s)) shall furnish agents of the (name the investigative agency/agencies) forthwith all information, facilities and technical assistance necessary to accomplish the installation of the (pen register) (and/or) (trap and trace device), including (the installation of Caller ID service on telephone number(s) _____ and) the installation and operation of the device(s), unobtrusively and with minimum interference to the services that are accorded persons whose telephone(s) is/are to be the subject of the device(s).

IT IS ORDERED FURTHER that the (name the investigative agency/agencies) will compensate the (name the communications service provider(s)) for expenses reasonably incurred in complying with this order.

IT IS ORDERED FURTHER that the results of the (pen register) (and/or) (trap and trace device) shall be furnished to the (name the investigative agency/agencies) at reasonable intervals during regular business hours for the duration of the order.

(In the case of a trap and trace, include the following:

IT IS ORDERED FURTHER that: (a) the tracing operations shall be limited to (Electronic Switching System (ESS)) or (No. 5 cross-bar switching facilities); and (b) the tracing operation shall be restricted to tracing and recording only those incoming electronic or other impulses originating from (identify the geographical area).)

IT IS ORDERED FURTHER, pursuant to Title 18, United States Code, Section 3123(d), that this order and the application be sealed until otherwise ordered by the Court, and that (name the communications service provider(s)), its agents and employees shall not disclose the existence of the (pen register) (and/or) (trap and trace device), the existence of this order, or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the Court.

UNITED STATES DISTRICT COURT JUDGE
(District)

_____ Date

Application for Video Surveillance

(FORM 15)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES FOR AN ORDER)
AUTHORIZING THE INTERCEPTION OF)
VISUAL, NON-VERBAL CONDUCT AND)
ACTIVITIES BY MEANS OF CLOSED)
CIRCUIT TELEVISION OCCURRING)
WITHIN THE PREMISES KNOWN AS)

_____)

APPLICATION FOR AN ORDER AUTHORIZING THE
INTERCEPTION OF VISUAL, NON-VERBAL CONDUCT AND
ACTIVITIES BY MEANS OF CLOSED CIRCUIT TELEVISION

A. Pursuant to Rule 41(b) of the Federal Rules of Criminal Procedure, the United States of America by and through _____, United States Attorney for the _____ District of _____, and _____, an Assistant United States Attorney for said District, hereby makes application to this Court for an order authorizing the interception and recording of visual, non-verbal conduct and activities by means of closed circuit television occurring within the following premises: (set forth a particularized description of the premises to be surveilled.) The factual basis for the granting of this application is set forth in the attached affidavit of _____, which is incorporated by reference herein.

B. Also attached to this application is a letter from the Director (or the Senior Associate Director or Associate Director), Office of Enforcement Operations, Criminal Division, United States Department of Justice, authorizing the making of this application for visual surveillance by means of closed circuit television.

C. The attached affidavit of _____ reflects that there is probable cause to believe:

1. The premises known as _____, located at _____, are being and will continue to be used by (name the interceptees), to commit offenses involving (list the violations).

2. The visual, non-verbal conduct and activities of the above-named individual(s) will be obtained through interception by means of closed circuit television at these premises and that such conduct and activities will provide:

a. information indicating the precise nature, scope, extent and methods of operation of the participants in the illegal activities referred to above,

b. information reflecting the identities and roles of accomplices, aiders and abettors, co-conspirators, and participants in the illegal activities referred to above, and

c. admissible evidence of commission of the offenses described above.

3. Installation of electronic visual surveillance equipment may require surreptitious entry into the premises (by breaking and entering, if necessary).

4. Normal investigative procedures have been tried and failed or reasonably appear unlikely to succeed, if tried, or appear to be too dangerous to employ.

5. On the basis of the attached affidavit of _____ and allegations contained in this application,

IT IS HEREBY REQUESTED that this Court authorize Special Agents of the (name the investigative agency/agencies) to intercept and record by means of closed circuit television visual, non-verbal conduct and activities of (name the interceptees) and others as yet unknown within the premises known as _____, located at _____, concerning offenses, involving (list the violations).

IT IS REQUESTED FURTHER that such interception not automatically terminate when the type of visual, non-verbal conduct described above has first been obtained but continue until conduct is intercepted that reveals: (1) the manner in which the above-named described offenses are being committed; (2) the precise nature, scope, and extent of the above-described offenses, and, (3) the identity and roles of accomplices, aiders and abettors, co-conspirators, and participants, or for a period of thirty (30) days from the date of this order, whichever is earlier.

IT IS REQUESTED FURTHER that Special Agents of the (name the investigative agency/agencies) be authorized to enter the above-described premises surreptitiously, covertly, and by breaking and entering, if necessary, in order to install, maintain and remove electronic visual surveillance equipment used by the (name the investigative agency/agencies) to intercept and

record visual, non-verbal conduct occurring within the foregoing premises.

IT IS REQUESTED FURTHER THAT this order require that it be executed as soon as practicable and that interception be conducted in such a manner as to minimize interception of visual, non-verbal conduct which is not criminal in nature, and that the order terminate upon attainment of the authorized objectives or at the end of thirty (30) days from the date of the order, whichever is earlier.

IT IS REQUESTED FURTHER that surveilling agents be authorized to spot monitor the premises to ascertain whether any of the aforementioned persons are present inside the premises.

When such persons are found to be present, the agents will continue the interception as to conduct that involves the designated offenses.

When it is determined that none of the named interceptees nor any person subsequently identified as an accomplice who uses the premises to commit or converse about the designated offense(s) is inside the premises, interception of visual, non-verbal conduct will be discontinued.

Dated: _____, 19__

Respectfully submitted,

Assistant United States Attorney

Order for Video Surveillance

(FORM 16)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES FOR AN)
ORDER AUTHORIZING THE INTERCEPTION)
OF VISUAL, NON-VERBAL CONDUCT)
AND ACTIVITIES BY MEANS OF CLOSED)
CIRCUIT TELEVISION OCCURRING)
WITHIN THE PREMISES KNOWN AS)

_____)

ORDER
AUTHORIZING THE INTERCEPTION OF VISUAL,
NON-VERBAL CONDUCT AND ACTIVITIES

Application under oath having been made before me by
_____, Assistant United States Attorney for the
_____ District, for an order authorizing the interception
and recording of visual, non-verbal conduct and activities
pursuant to Rule 41(b) of the Federal Rules of Criminal Procedure
and full consideration having been given to the matters set forth
therein, the Court finds:

A. There is probable cause to believe that
_____ and others as yet unknown have committed and
are committing offenses involving (list the offenses).

B. There is probable cause to believe that particular
visual, non-verbal conduct and activities concerning these
offenses will be obtained through the interception for which
authorization is herewith applied. In particular, visual,
non-verbal conduct and activities will concern the (characterize
the offenses).

C. Normal investigative procedures have been tried and
failed, reasonably appear unlikely to succeed if tried or
continued, or are too dangerous.

D. There is probable cause to believe that the premises
(located at) (known as) _____ have been and are
being used by _____ and others as yet
unknown, in connection with the commission of the above-stated
offenses.

WHEREFORE, IT IS HEREBY ORDERED that the (name of the investigative agency/agencies) is authorized, to intercept and record the visual, non-verbal conduct and activities of (name interceptees) and others as yet unknown, concerning the above-described offenses at the premises located at _____). Such interception shall not terminate automatically when the type of conduct/ activity described above in paragraph (B) has first been observed but shall continue until the conduct or activity is intercepted that reveals the manner in which (name the interceptees), and others as yet unknown participate in the specified offenses and reveals the identities of (his)(their) coconspirators, their methods of operation, and the nature of the conspiracy, or for a period of (state the time period not to exceed 30 days), whichever is earlier.

IT IS ORDERED FURTHER that special agents of the (name of the investigative agency/agencies) are authorized to enter the foregoing premises surreptitiously for the purpose of installing, maintaining, and removing any electronic monitoring devices utilized pursuant to the authority granted by this order.

PROVIDING THAT, this authorization to intercept visual, non-verbal conduct and activities shall be executed as soon as practicable after the signing of this order and shall be conducted in such a way as to minimize the interception of conduct and activities not otherwise subject to interception, and must terminate upon attainment of the authorized objective or, in any event, at the end of (not to exceed 30) days.

JUDGE

Date: _____

Application for Disclosure

(FORM 17)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING THE)
DISCLOSURE OF INTERCEPTED WIRE, ORAL)
AND/OR ELECTRONIC COMMUNICATIONS.)

APPLICATION

_____, an Attorney for the United States
Department of Justice (or an Assistant United States Attorney)
states:

A. I am an "investigative or law enforcement officer of
the United States" within the meaning of 18 U.S.C. § 2510(7),
that is, an attorney authorized by law to prosecute violations of
federal law.

B. I am also an "attorney for the government" as defined
in Rule 54(c) of the Federal Rules of Criminal Procedure, and,
therefore, pursuant to 18 U.S.C. § 2516(1) and (3) and 18 U.S.C.
§ 2518(8)(b), am authorized to make application to a federal
judge of competent jurisdiction for authorization to disclose the
application, order and contents of intercepted wire, oral and/or
electronic communications upon a showing of good cause pursuant
to 18 U.S.C. § 2518(8)(b).

C. This application seeks authorization to disclose
intercepted wire, oral and/or electronic communications of (name
of the interceptee(s)) relating to felony violations of federal
law, that is violations of (characterize the offenses) which were
intercepted pursuant to a court order issued by Judge
_____ of this court on the _____ day of _____,
19___. Extensions of said order were issued on (use, if
appropriate). The order was terminated on the _____ day of
_____, 19___. The tapes herein were sealed pursuant
to order of the court on the _____ day of _____, 19__.

(If appropriate, state: "The tapes were unsealed on the ____
day of _____, 19__, by order of the court in

connection with the litigation of (name the case) and resealed on the _____ day of _____, 19__.

1) The wire communications were intercepted over telephone _____, located at _____, subscribed to by _____, and/or _____.

2) Electronic communications were intercepted over (describe the facility) listed in the name of _____ and located at _____, and/or _____.

3) Oral communications were intercepted at (identify the location) owned or leased by _____.

D. Disclosure of the intercepted wire, oral and/or electronic communications is sought in connection with

(Here describe the reason(s) for disclosure and the proceeding in which the intercepted communications will be disclosed.)

Attached is the affidavit of (indicate the affiant's name and agency) setting forth a complete statement of facts which, in the opinion of the applicant, provide good and sufficient cause for the disclosure of the intercepted communications pursuant to 18 U.S.C. § 2518(8) (b).

E. Based on my knowledge, information and belief, I know of no previous application for the relief sought herein having been made to any judge or court except as is set forth herein.

(If a prior application was made for disclosure, it should be set forth here and reflect the action of court)

F. On the basis of the facts set forth in the affidavit of (specify the agent) accompanying this application and attached hereto, the applicant requests this court to issue an order, pursuant to the authority conferred on it by 18 U.S.C. § 2518(8) (b) authorizing the disclosure of the wire, oral and/or electronic communications described herein in connection with the proceeding heretofore described.

G. Use only if appropriate, the following: "The applicant requests further that the order incorporate the following limitations on disclosure in order to protect the rights of confidential sources or innocent third parties."

(Describe here the limitations that should be placed on the disclosure, if any, and give the reasons.)

H. I request further that the court order indicate that this order does not affect any lawful disclosures that could otherwise be made pursuant to the provisions of 18 U.S.C. § 2517.

I declare under penalty of perjury pursuant to 28 U.S.C. § 1746 that the foregoing is true and correct to the best of my knowledge, information and belief.

Executed on _____, 19__.

Applicant

Order for Disclosure of Interceptions

(FORM 18)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

) IN THE MATTER OF THE)
) APPLICATION OF THE UNITED)
) STATES FOR AN ORDER)
) AUTHORIZING THE DISCLOSURE)
) OF INTERCEPTED WIRE, ORAL)
) AND/OR ELECTRONIC COMMUNICATIONS)

ORDER AUTHORIZING THE DISCLOSURE OF
INTERCEPTED WIRE, ORAL AND/OR ELECTRONIC
COMMUNICATIONS

Application under penalty of perjury having been made before me by _____, an "investigative or law enforcement officer" as defined in 18 U.S.C. § 2510(7) and an "attorney for the government" as defined in Rule 54(c) of the Federal Rules of Criminal Procedure, for an order authorizing the disclosure of applications, orders and intercepted communications, intercepted pursuant to 18 U.S.C. § 2510 et seq. and full consideration having been given to the matters set forth herein, the court finds:

A. There is good and sufficient cause to disclose wire, oral and/or electronic communications of (name the interceptee(s)) intercepted during the period (set forth period in question) over facilities (here describe wire, oral or electronic facilities), pursuant to an order of this court on the _____ day of _____ 19 _____, for use in connection with _____

(Here, describe the proceedings they are to be disclosed in connection with.)

B. (Use only if appropriate) To protect the identity of confidential sources and innocent third parties the following restrictions are placed on this disclosure unless and until further ordered by the court:

Disclosure is not be made with regard to
(here place restrictions, if any. Clarify exact
information sought to be restricted.)

C. Nothing in this order shall affect the disclosure of information relating to intercepted communications, the disclosure of which would otherwise be lawful under 18 U.S.C. § 2517.

Wherefore, it is hereby ordered that (subject to the restrictions set forth herein) (name the investigative agency/agencies) is authorized, pursuant to an application made by (applicant) pursuant to authority set forth in 18 U.S.C. §§ 2516(1) and (3) and 2518(8)(b) to disclose intercepted wire, oral and/or electronic communications in connection with the proceedings heretofore described.

UNITED STATES DISTRICT COURT JUDGE

(Date)

Section 2517(5) Application for Testimonial Use
of Interceptions Relating to "Other Offenses"

(FORM 19)

UNITED STATES DISTRICT COURT

DISTRICT OF _____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES FOR AN ORDER) No. _____
AUTHORIZING THE INTERCEPTION OF)
(WIRE/ORAL/ELECTRONIC)
COMMUNICATIONS))

APPLICATION FOR AN ORDER AUTHORIZING THE
DISCLOSURE AND USE OF INTERCEPTED COMMUNICATIONS
PURSUANT TO SECTION 2517(5), TITLE 18, UNITED STATES CODE

_____, [an Assistant United States Attorney
for the _____ District of _____,]⁸ being
duly sworn, states:

This application is submitted in support of a request for an Order pursuant to the provisions of Title 18, United States Code, Section 2517(5), authorizing the disclosure and use of communications intercepted pursuant to the provisions of Chapter 119, Title 18, United States Code as evidence, while giving testimony under oath, as authorized in Section 2517(3), Title 18 United States Code, in any proceeding held under the authority of the United States relating to a prosecution for violations of Section [], Title 18, United States Code, relating to (describe the offense(s)) and in support thereof states as follows:

1) I am an "investigative or law enforcement officer of the United States" within the meaning of Section 2510(7), Title 18, United States Code -- that is, (s)he is an attorney authorized by law to prosecute or participate in the prosecution of offenses enumerated in Section 2516, Title 18, United States Code:

2). On _____, United States District Judge
_____, _____ District of _____,
entered an order in (specify the case number), authorizing
Special Agents of the (identify the investigative
agency/agencies) to intercept for a _____ day period

⁸ In the alternative, state "an attorney of the United States Department of Justice," if the applicant is a Criminal Division attorney.

(wire/oral/electronic) communications of _____,
_____ and others as yet unknown
(over the telephone(s) (or facsimile machine/pager) bearing the
number(s) _____, and _____
listed to _____, at _____) and/or (occurring
at the premises known as _____, located at
_____) for the purpose of obtaining evidence concerning
the commission of offenses enumerated in Section 2516 of Title
18, United States Code, that is, Title _____, United States
Code, Sections _____, _____, and _____.

3) During the course of the electronic surveillance authorized under the orders referred to above were communications which relate to allegations that (give a general description of conduct constituting offense), in that (describe the general contents of the conversations which are to be used). These communications were intercepted incidentally and in good faith during the course of the electronic surveillance which was conducted in accordance with the provisions of Chapter 119, Title 18, United States Code.

4) (if applicable) Among the evidence introduced at the trial of the case entitled _____ were recordings of communications intercepted pursuant to the authorization(s) referred to above.

5) (if applicable) On _____, the Honorable _____ entered an order finding that the interceptions made during the course of the electronic surveillance authorized pursuant to the orders referred to above were made pursuant to the provisions of Chapter 119, Title 18, United States Code.

WHEREFORE, on the basis of the allegations set forth above, applicant requests that the Court enter an Order authorizing the disclosure and use of the contents of communications intercepted pursuant to the orders referred to above and evidence derived therefrom while giving testimony under oath or affirmation in any proceeding held under the authority of the United States in connection with any prosecution for violations of Title 18, United States Code, Sections [].

UNITED STATES ATTORNEY

Assistant United States Attorney

9 Set forth a separate paragraph for each separate order authorizing the interception of communications.

Section 2517(5) Order Permitting Testimonial Use
of Interceptions Relating to "Other Offenses"

(FORM 20)

UNITED STATES DISTRICT COURT

DISTRICT OF _____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES FOR AN ORDER)
AUTHORIZING THE INTERCEPTION OF)
(WIRE/ORAL/ELECTRONIC))
COMMUNICATIONS)

No. _____

O R D E R

Application under oath having been made before me for an order pursuant to Section 2517(5) of Title 18, United States Code, by the United States by its attorney _____, Assistant United States Attorney for the _____ District of _____, an "investigative or law enforcement officer of the United States" as defined in Section 2510(7) of Title 18, United States Code, I FIND that:

1) On _____, United States District Judge _____, District of _____, entered an order in case no. _____ authorizing Special Agents of the (identify the investigative agency/agencies) to intercept for a _____ day period (wire/oral/electronic) communications of _____, and others as yet unknown over (the telephones/pagers/facsimile machines bearing the number(s) _____ and _____ listed to _____, at _____, for the purpose of obtaining evidence concerning the commission of offenses specified in Section 2516 of Title 18, United States Code, that is Title 18, United States Code Sections _____, _____, and _____.

2) During the period of authorized interception, (wire/oral/electronic) communications were intercepted in accordance with the provisions of Chapter 119, Title 18, United States Code, which were pertinent to the authorized objectives specified in the interception.

3) During the period of interception communications were also intercepted, in accordance with the provisions of Chapter 119, Title 18, United States Code, incidentally and in good faith, which may be pertinent to a prosecution for a violation of

¹ Prepare a separate paragraph for each order.

Title 18, United States Code, Section(s) [] relating to
(provide a description of the offense(s)).

WHEREFORE, It is ORDERED, pursuant to the provisions of Section 2517(5), Title 18, United States Code, that any person who has received, by any means authorized by Chapter 119, Title 18, United States Code, any information concerning the (wire/oral/electronic) communications intercepted pursuant to the authorizations specified in paragraph(s) 1, __, and __ above, or evidence derived therefrom, may disclose and use the contents of said communications, and evidence derived therefrom, while giving testimony under oath or affirmation in any proceeding held under the authority of the United States in connection with a prosecution for a violation of Title 18, United States Code, Section(s) [].

Date: _____

UNITED STATES DISTRICT COURT JUDGE

Inventory Application

(FORM 21)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AN ORDER AUTHORIZING THE
INTERCEPTION OF WIRE¹ COMMUNICATIONS

TO AND FROM TELEPHONE NUMBER ()

_____, SUBSCRIBED TO BY

_____ and located at

LIST OF PERSONS NAMED IN AUTHORIZATION ORDERS
AND OTHERS WHOSE WIRE COMMUNICATIONS WERE INTERCEPTED

In order to assist the Court in making its determination of those persons to be served with inventories as provided by Title 18, United States Code, Section 2518(8)(d) in the above matter, the Government respectfully submits this compilation of the names of those persons named in the applications and court orders and other persons who have been identified by the (name the investigative agency/agencies) as persons whose wire communications were intercepted:

1. The persons named in the application and orders are:
(name) (address)

2. The persons whose wire communications were intercepted and who have been identified by the (name the agency/agencies) are:

See attached list.

3. In addition to the persons specified above, numerous communications of persons as yet unidentified were intercepted. In the event that any such persons are later identified, a supplemental list will be submitted to the Court.

Dated:

Assistant United States Attorney

¹ This is just an example; inventory notice must also be sent to those individuals whose oral and electronic communications were intercepted.

Order for Inventory

(FORM 22)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AN ORDER AUTHORIZING THE
INTERCEPTION OF WIRE COMMUNICATIONS
TO AND FROM TELEPHONE NUMBER
() _____, SUBSCRIBED TO
BY _____ AND LOCATED AT

ORDER AND INVENTORY

TO: ATTORNEYS OF THE UNITED STATES DEPARTMENT OF JUSTICE

Having examined the Government's list of (a) persons named in the captioned applications and orders authorizing the interception of wire communications and (b) others thus far identified as persons whose wire communications were intercepted pursuant to those orders, pursuant to Title 18, United States Code, Section 2518(8)(d),

IT IS HEREBY ORDERED that attorneys for the United States Department of Justice shall cause to be served upon the persons listed on the annexed list an inventory which shall include notice of:

1. The fact of the entry of the orders described above authorizing the interception of wire communications.
2. The fact that the period of authorized interception pursuant to those orders included the periods between _____ and _____, 199____, and _____ and _____, 199____, by on or about which date all original recordings were sealed by order of this court.
3. The fact that during the period of authorized interception, wire communications were or were not intercepted.

The persons to be served are set forth on the attached list.

UNITED STATES DISTRICT JUDGE

(FORM 23)

UNITED STATES DISTRICT COURT
DISTRICT OF

() _____, SUBSCRIBED TO BY)
AND LOCATED AT)

1. On _____, 19__ and _____, 19__,
the Honorable _____ authorized the interception
of wire communications over the above-captioned telephone.

2. The period of authorized interception pursuant to those orders included the periods between _____ and _____, 19____, and _____ and _____, 19____, by on or about which date all original recordings were sealed by order of this Court.

3. During the period of authorized interception, wire communications to or from your telephone were intercepted (and/or your wire communications were intercepted).

Dated:

(INVESTIGATIVE AGENCY):

Application for Destruction of Tapes

(FORM 24)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

IN THE MATTER OF THE)
APPLICATION OF THE UNITED)
STATES FOR AN ORDER)
AUTHORIZING THE DESTRUCTION)
OF INTERCEPTED WIRE, ORAL)
AND/OR ELECTRONIC COMMUNICATIONS)

APPLICATION

_____, an attorney of the United States Department of Justice or (Assistant United States Attorney) states:

I am an "investigative or law enforcement officer of the United States" within the meaning of 18 U.S.C. § 2510(7), that is, an attorney authorized by law to prosecute violations of federal law.

I am also an "attorney for the government" as defined in Rule 54(c) of the Federal Rules of Criminal Procedure and, therefore, pursuant to 18 U.S.C. §§ 2516(1) and (3), and 2518(8)(a), am authorized to make application to a federal judge of competent jurisdiction for authorization to destroy the original tapes of wire, oral and/or electronic communications seized pursuant to a lawful court order, in compliance with 18 U.S.C. 2518(8)(a).

This application seeks authorization to destroy the original tapes of wire, oral and/or electronic communications of (name the interceptee(s)) relating to felony violations of federal law, that is violations of (characterize the offenses) which were intercepted pursuant to a court order issued by Judge _____ of this court on the _____ day of _____ 19__.

Extensions of said order were issued on _____. The order was terminated on the _____ day of _____ 19__. The tapes herein were sealed pursuant to the order of the court on the _____ day of _____ 19__.

The tapes were subsequently unsealed pursuant to court order on the _____ day of _____ 19__, in connection with the (name of the prosecution or other reason for unsealing).

The tapes were resealed pursuant to court order on the _____ day of _____ 19__.

(Use the following language as appropriate.)

1. The wire communications were intercepted over telephone number _____ located at _____ and subscribed to by _____.

2. Electronic communications were intercepted over (describe the facility/facilities) listed in the name of _____ and located at _____.

3. Oral communications were intercepted at (specify the location) owned or leased by _____.

(Use the following language as appropriate.)

At the time of sealing, Judge _____ ordered (identify the custodial agency) to maintain custody of the intercepted communications.

A period of ten years has elapsed since the tapes were sealed by order of Judge _____. According to my knowledge, information and belief, all prosecutions in connection therewith are terminated and there is no further need or legal reason to maintain the tapes. The investigating agency involved, (name of the agency), concurs in this application.

On the basis of the facts set forth in this application, the applicant requests that the court issue an order authorizing the destruction of the wire, oral and/or electronic communications described herein.

I declare under penalty of perjury pursuant to 28 U.S.C. § 1746 that the foregoing is true and correct to the best of my knowledge, information and belief.

Executed on the _____ day of _____ 19 _____.

Applicant

Order for Destruction of Tapes

(FORM 25)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

IN THE MATTER OF THE)
APPLICATION OF THE UNITED)
STATES FOR AN ORDER)
AUTHORIZING THE DESTRUCTION)
OF INTERCEPTED WIRE, ORAL)
AND/OR ELECTRONIC COMMUNICATIONS)

ORDER AUTHORIZING THE DESTRUCTION OF
INTERCEPTED WIRE, ORAL AND/OR ELECTRONIC
COMMUNICATIONS

Application under penalty of perjury having been made before me by _____, an "investigative or law enforcement officer" as defined in 18 U.S.C. § 2510(7) and an "attorney for the government" as defined in Rule 54(c) of the Federal Rules of Criminal Procedure, for an order authorizing the destruction of intercepted wire, oral and/or electronic communications, intercepted pursuant to 18 U.S.C. § 2510 et seq. and full consideration having been given to the matters set forth herein, the court finds:

On the _____ day of _____, 19____, an order for the interception of wire, oral, and/or electronic communications was issued by Judge _____ of this district to intercept the communications of (identify the principal person(s) and others) (over telephone number _____) located at _____ and subscribed to by _____ or (at the premises described as _____ and owned by or leased to _____) (If electronic communications were intercepted, a description of the facilities, the subscriber and the location should be set forth.) in connection with violations of _____ (specify the principal federal statutory violations). Extensions of the original order were issued on (specify the dates) by (identify the judge). The interceptions were terminated on the _____ day of _____, 19____. The intercepted communications were sealed by the court on the _____ day of _____, 19____.

The intercepted communications were subsequently used in the prosecution of (name the cases).

The tapes were unsealed pursuant to court order on _____ and resealed on _____ (use, if appropriate).

Ten years having elapsed from the time the tapes were originally sealed pursuant to 18 U.S.C. § 2518(8)(a), and there appearing to be no further need for their retention,

IT IS HEREBY ORDERED that the above-described intercepted wire, oral and/or electronic communications be destroyed by (identify the agency having possession), the lawful custodian designated by the issuing judge.

Judge

Affidavit for Mobile Tracking Device

(FORM 26)

UNITED STATES DISTRICT COURT
DISTRICT OF _____

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AN ORDER AUTHORIZING THE
MONITORING OF A MOBILE TRACKING
DEVICE IN OR ON A _____,

LICENSE PLATE NUMBER _____,
VEHICLE IDENTIFICATION NUMBER _____.

APPLICATION TO
MONITOR A MOBILE
TRACKING DEVICE.

(Fed. R. Crim. P. 41;
18 U.S.C. § 3117)

_____ DISTRICT OF _____, SS:

_____, being duly sworn, deposes and says that I am
a Special Agent with the _____, duly
appointed according to law and acting as such.

Upon information and belief, a _____,
license plate number _____, vehicle identification
number _____ ("the subject vehicle"), is presently being
used in a conspiracy to (identify the offense(s)).

Your deponent further states that there is probable cause to
believe that the installation of a mobile tracking device placed
in or on the subject vehicle, and monitoring of the mobile
tracking device, will lead to evidence of the aforementioned
conspiracy to distribute narcotics as well as to the
identification of individuals who are engaged in the commission
of that and related crimes.

The source of your deponent's information and the grounds
for his belief are as follows:

1. I have been a Special Agent with the _____
for _____ years, and am the case agent on this case. As the case
agent, I am fully familiar with the facts of the case.

2. On or about _____, I learned
from a reliable confidential informant ("CI") that _____
was involved in (list the offense(s)) in (location). The CI
subsequently informed me that _____.

3. On _____, at approximately _____, I established a
surveillance in the vicinity of _____. I

observed _____ leave a building located at _____ and enter the subject vehicle.

4. A review of Department of Motor Vehicles records reveals that the subject vehicle is registered to _____.

5. The CI has stated that _____ is using the subject vehicle in connection with (describe the criminal activity). Based upon my own observations, I know that the subject vehicle is presently within the _____ District of _____.

6. In order to track the movement of the subject vehicle effectively and to decrease the chance of detection, I seek to place a mobile tracking device in or on the subject vehicle while it is in the _____ District of _____. Because _____ sometimes parks the subject vehicle in his driveway and on other private property, it may be necessary to enter onto private property in order to effect the installation of the mobile tracking device.

7. In the event that the Court grants this application, there will be periodic monitoring of the mobile tracking device during both daytime and nighttime hours for the next 10 days. In addition, the mobile tracking device may produce signals from inside private garages or other such locations not open to public or visual surveillance.

8. In light of the nature of this affidavit, I request that it be sealed.

WHEREFORE, your deponent respectfully requests that the Court issue an order authorizing members of _____ or their authorized representatives, including but not limited to other law enforcement agents and technicians assisting in the above-described investigation, to install a mobile tracking device in or on the subject vehicle; to enter onto private property to effect said installation; to surreptitiously enter the vehicle to effect said installation; and to monitor the signals from that tracking device, for a period of 10 days following the issuance of the Court's order, including signals produced from inside private garages and other locations not open to the public or visual surveillance, and signals produced in the event that the subject vehicle leaves the _____ District of _____ but remains within the United States.

Special Agent

Sworn to before me this _____ day of _____, _____

Order for Mobile Tracking Device

(FORM 27)

UNITED STATES DISTRICT COURT

DISTRICT OF _____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING THE)
MONITORING OF A MOBILE TRACKING)
DEVICE IN OR ON A _____,)

LICENSE PLATE NUMBER _____,)
VEHICLE IDENTIFICATION NUMBER _____)

_____)
_____)

ORDER TO
MONITOR A MOBILE
TRACKING DEVICE

(Fed. R. Crim. P. 41;
18 U.S.C. § 3117)

DISTRICT OF _____, SS:

WHEREAS an affidavit has been presented to the Court by
Special Agent _____ of the _____,
and full consideration having been given to the matters set
forth therein, this Court finds that there is probable cause to
believe that monitoring of a mobile tracking device placed
on a private vehicle described as a _____,
_____ license plate number _____, vehicle identification
number _____ ("the subject vehicle"), will lead to
evidence of violations of (state the offenses). Therefore, it is

ORDERED, pursuant to Fed. R. Crim. P. 41 and 18 U.S.C. §
3117, that Special Agent _____ of the _____,
together with other Special Agents and their authorized
representatives are authorized, within ten days from the date of
this order, to install in or on the subject vehicle, which is
presently located in the _____ District of _____, a
mobile tracking device; it is further

ORDERED that said Special Agents and their authorized representatives are further authorized to enter onto private property and surreptitiously to enter said vehicle to effect the installation of the mobile tracking device; it is further

ORDERED that said Special Agents and their authorized representatives are authorized, for a period of ten days from the date of this order, to monitor the signals from the mobile tracking device, including those signals produced from inside any private garage or other location not open to public or visual surveillance, and, in the event the subject vehicle travels outside the _____ District of _____, those signals produced outside the _____ District of _____ but within the United States; and it is further

ORDERED that this application and the Affidavit of Special Agent _____ be sealed until further order of the Court.

Dated:

UNITED STATES MAGISTRATE JUDGE
(District)